Cisco Prime Network Control System Configuration Guide

Software Release 1.1
May 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25451-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Copyright © 2012 Cisco Systems, Inc.
All rights reserved.

CONTENTS

Preface

The preface provides an overview of the *Cisco Prime Network Control System Configuration Guide, Release 1.1*, references related publications, and explains how to obtain other documentation and technical assistance, if necessary. This chapter contains the following sections:

Audience

This guide describes the Cisco Prime Network Control System (NCS). It is meant for networking professionals, who use the NCS to manage a Cisco Unified Network Solution. To use this guide, you should be familiar with the concepts and terminology associated with wired and wireless LANs.

Purpose

This guide provides the information you need to manage a Cisco Unified Network Solution using the NCS.

Note This guide pertains specifically to NCS Release 1.1. Earlier versions of NCS or WCS software might look and operate somewhat differently.

Conventions

This publication uses the following conventions to convey instructions and information:

- Commands and keywords are in **boldface** text.
- Variables are in *italicized* text.
- Examples depict screen displays and the commandline in `screen` font.

- Information you need to enter in examples is shown in **`boldface screen`** font.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not contained in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Publications

For more information about the NCS and related products, see the following URL:

http://www.cisco.com/cisco/web/psa/default.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Cisco NCS Overview

This chapter describes the Cisco Unified Network Solution and the Cisco Prime Network Control System (NCS). It contains the following sections:

The Cisco Unified Network Solution

The Cisco Unified Network Solution provides both wired and 802.11 wireless networking solutions for enterprises and service providers. It simplifies the deployment and management of large-scale wired and wireless LANs and enables you to create a unique best-in-class security infrastructure. The operating system manages all client data, communications, and system administration functions, performs Radio Resource Management (RRM) functions, manages system-wide mobility policies using the operating system security solution, and coordinates all security functions using the operating system security framework.

The Cisco Unified Network Solution consists of Cisco Managed Switches, Cisco Unified Wireless Network Controllers (hereafter called *controllers*), and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the following operating system user interfaces:

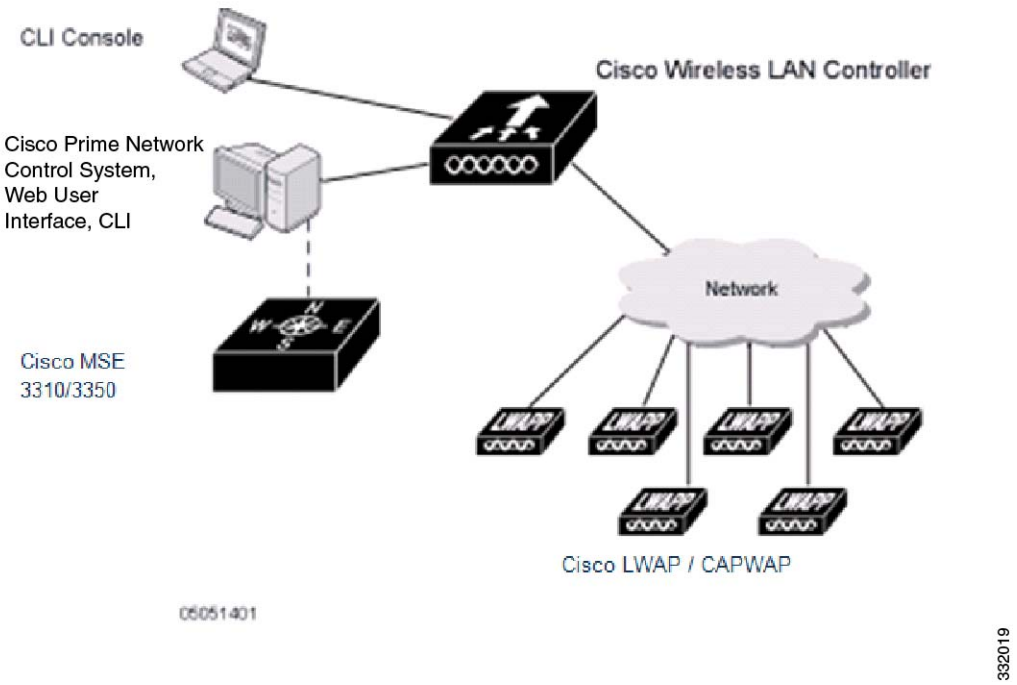
- An HTTPS full-featured web user interface hosted by Cisco controllers can be used to configure and monitor individual controllers.
- A full-featured command-line interface (CLI) can be used to configure and monitor individual controllers.
- NCS can be used to configure and monitor one or more controllers and associated access points. NCS has tools to facilitate large-system monitoring and control. It runs on predefined physical appliances and on specific virtual deployments.
- An industry-standard SNMP V1, V2c, and V3 interface can be used with any SNMP-compliant third-party network management system.

The Cisco Unified Network Solution supports client data services, client monitoring and control, and all rogue access point detection, monitoring, and containment functions. It uses lightweight access points, controllers, and the optional NCS to provide wireless services to enterprises and service providers.

Note Unless specified otherwise, information pertaining to controllers applies to all Cisco Unified Wireless Network Controllers, including but not limited to Cisco 2000 and 2100 Series Unified Wireless Network Controllers, Cisco 4100 Series Unified Wireless Network Controllers, Cisco 4400 Series Unified Wireless Network Controllers, Cisco 5500 Series Wireless LAN Controllers, and controllers within the Cisco Wireless Services Module (WiSM) and Cisco 26/28/37/38*xx* Series Integrated Services routers.

Figure 1-1 shows the Cisco Unified Network Solution components, which can be simultaneously deployed across multiple floors and buildings.

Figure 1-1 Cisco Unified Network Solution



About the NCS

The NCS is a Cisco LAN Solution network management tool that adds to the capabilities of the web user interface and the command-line interface (CLI). NCS enables you to manage a network of controllers.

NCS enables you to configure and monitor one or more controllers, switches and associated access points. NCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.

On Linux, NCS runs as a service, which runs continuously and resumes running after a reboot.

The NCS user interface requires Mozilla Firefox 3.6 or later or Internet Explorer 8 with the Chrome plugin releases or Google Chrome 12.0.742.x. The administrator defines permissions from the Administration menu, which also enables the administrator to manage user accounts and schedule periodic maintenance tasks.

Note We strongly recommend that you do not enable third-party browser extensions. In Internet Explorer, you can disable third-party browser extensions by choosing **Tools > Internet Options** and unselecting the **Enable third-party browser extensions** check box on the Advanced tab.

NCS simplifies controller configuration and monitoring and reduces data entry errors. NCS uses the industry-standard SNMP protocol to communicate with the controllers.

NCS also includes the Floor Plan editor, which allows you to do the following:

- Access vectorized bitmap campus, floor plan, and outdoor area maps.
- Add and change wall types.
- Import the vector wall format maps into the database.

Note The vector files allow the Cisco NCS RF Prediction Tool to make better RF predictions based on more accurate wall and window RF attenuation values.

NCS Licenses

NCS is deployed through physical or virtual appliances; you use the standard License Center Graphical User Interface to add new licenses, which is locked by the standard Cisco Unique Device Identifier (UDI). When NCS is deployed on a virtual appliance, the licensing is similar to a physical appliance, except instead of using a UDI, you use a Virtual Unique Device Identifier (VUDI).

Note If you want to move licenses from one physical appliance to another, you need to call the Cisco TAC and rehost the licenses to a new UDI.

The NCS license is recognized by the SKU, which is usually attached to every purchase order to clearly identify which software or package is purchased by a customer. The different NCS license options are described in this section. This section contains the following topics:

NCS Evaluation License

NCS can be used in a lab or in an evaluation with the following license: NCS-DEMO-10. This license provides an evaluation license for 10 devices, and for a duration of 30 days. If you need a custom device count or duration, please contact your Cisco representative.

NCS Device Count License

NCS uses a single-tier licensing structure that includes all features and functionality in a single tier. Part numbers are purchased based on number of devices to be managed. Part numbers are available to support 50, 100, 500, 1000, 2500, 5000 or 10000 devices; where both an AP and a Switch are considered a single, managed device.

The NCS Device Count license allows you to either choose a physical appliance or virtual appliance for the NCS setup. If you choose the option of ordering the physical appliances, the PRIME-NCS-APL-K9 is shipped to you along with a PAK for the license quantity you ordered. That is, if you are ordering L-NCS-1.1-1K with PRIME-NCS-APL-K9 SKU, you get a physical NCS appliance, plus a PAK for managing 1000 devices.

If you choose the virtual appliance option, you download the virtual NCS image and the L-NCS-1.1-X PAK is mailed to you once it has been ordered.

If you want to add more devices to your network, you can get the L-NCS-1.1-X-ADD SKU for X devices. The L-NCS-1.1-X-ADD are identical licenses supplied. The only difference is that these SKUs are for additional licenses and they do not come with physical or virtual activation.

The larger license quantities, specifically 1K, 2.5K, 5K, and 10K are shipped in smaller increments to allow the licenses to be split across different NCS instances.

NCS Upgrade License

The L-NCS-2.0-UPGRADE-X-ADD SKU is used to upgrade NCS 1.X to NCS 2.X. Upgrades come in the following counts: 50, 100, and 500, 1K, 2.5K, 5K and 10K devices.

Once the lower-license level count is equaled or exceeded, the system considers the license for the next level. At this point new, lower-level licenses are not allowed, but additional higher-level licenses are allowed.

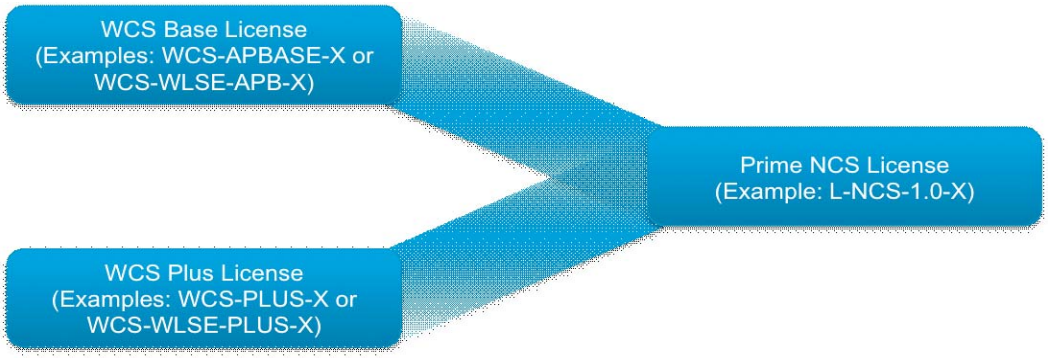
Note that a higher-level system allows lower-level licenses as long as there is no higher-level license or upgrade license present. This allows you to migrate licenses; take care to migrate the licenses in order from the lowest version to the highest version.

Consider a case where you are running NCS 3.0 and you have NCS 1.0, NCS 2.0, and NCS 3.0 licenses. You need to replace the current appliance with a new one and want to move the licenses, but not as part of a backup/restore process. You must first load all NCS 1.0 licenses, an NCS 2.0 Upgrade, the NCS 2.0 licenses, an NCS 3.0 Upgrade, and then all the NCS 3.0 licenses for the licenses to be applied correctly.

NCS Migration License

The NCS uses a single-tier license model. When Cisco WCS BASE or WCS PLUS licenses are being migrated, licenses mapped to the new Cisco Prime NCS single-tier model. This is a two-stage process.

This section contains the following topics:



The migration licenses that are generated from the Cisco migration portal basically have two levels of plus or base license with a count, additionally there can be a spectrum expert license. These licenses are mapped to NCS 1.1 licenses of equivalent counts. For example, a WCS 7.0 Base 500 with Spectrum Expert licenses can be converted to an NCS 1.1 500 device license.

Obtaining the XML File from the Existing WCS Deployment

Note Before adding the licenses that are migrated from your WCS installation, apply the L-WCS-NCS1-M-K9 license. The licenses migrated from WCS are generated as "ADD" licenses, and you cannot apply them unless you apply the L-WCS-NCS1-M-K9 license.

To Obtain the XML file from the existing WCS deployment, follow these steps:

Step 1 Log in to the WCS server (Version 7.0.164.0 or later) and choose **Administration > License Center**.

Step 2 From the left sidebar menu, choose **File > WCS File**.

Step 3 Select the WCS license you want to export, and click the **Export** button and save the XML file generated to your local machine.

Uploading the XML File to the Cisco Migration Portal

To upload the generated XML file to the Cisco Migration Portal, follow these steps:

Step 1 Go to: http://www.cisco.com/go/license

Step 2 Scroll down to the Migration section and click the **Register for Upgrade/Migrate License** link.

Step 3 Choose **NCS 1.0** from the drop-down list, and click **Go to Upgrade/Migration License Portal**.

Step 4 Enter your Product ID and Serial Number.

Step 5 Open the generated XML file in a text editor and copy the contents of the file to the License text box.

Step 6 Accept the end-user license agreement (EULA), verify your contact information, and click **Continue**.

Step 7 The Cisco Migration Portal generates and e-mails the new license file to you.

Note To apply the license to NCS, you must have the Network Control System license key file to install your license. The key file is distributed to you in an e-mail message from Cisco Systems. Do not edit the contents of the.lic file in any way or you might corrupt the file.

Cisco Unified Network Components

Cisco Unified Network Solutions ensures that your business achieves the highest level of network security and versatility. Cisco Unified Network Solutions empowers your network with the ability to offer secure wireless networking, either within your office for increased mobility or bridging between your office buildings. This section describes the different network components in the Cisco Unified Network Solutions and contains the following topics:

Cisco Prime NCS

With NCS, network administrators have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and wired and wireless LAN systems management. Robust graphical interfaces make wired and wireless LAN deployment and operations simple and cost-effective. Detailed trending and analysis reports make NCS vital to ongoing network operations.

WLAN Controllers

The WLAN controllers are highly scalable and flexible platforms that enables system wide services for mission-critical wireless in medium to large-sized enterprises and campus environments. Designed for 802.11n performance and maximum scalability, the WLAN controllers offer enhanced uptime with the ability to simultaneously manage from 5000 access points to 250 access points; superior performance for reliable streaming video and toll quality voice; and improved fault recovery for a consistent mobility experience in the most demanding environments.

NCS supports the Cisco wireless controllers that help reduce the overall operational expense of Cisco Unified Networks by simplifying network deployment, operations, and management. The following WLAN controllers are supported in NCS:

- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 2500 Series Wireless Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless Controllers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches

- Cisco Wireless Services Module 2 (WiSM2) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless Controller on SRE for ISR G2 Routers
- Cisco Flex 7500 Series Wireless Controllers
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers

Access Points

NCS supports the industry-leading performance access points for highly secure and reliable wireless connections for both indoor and outdoor environments. NCS supports a broad portfolio of access points targeted to the specific needs of all industries, business types, and topologies.

The following access points are supported in NCS:

- Cisco Aironet 801, 802, 1000, 1040, 1100, 1130, 1140, 1200, 1230, 1240, 1250, 1260, 1310, 1500, 1524, 1552, 3500i, 3500e, 3500p, 3600i, and 3600e Series Lightweight Access Points.
- Cisco Aironet 1040, 1100, 1130, 1141, 1142, 1200, 1240, 1250, and 1260 Autonomous Access Points.
- Cisco 600 Series OfficeExtend Access Points.
- Cisco Aironet Access Points running Lightweight Access Point Protocol (LWAPP) or Control and Provisioning of Wireless Access Points (CAPWAP) protocol.

Embedded Access Points

NCS supports the AP801, which is the integrated access point on the Cisco 800 Series Integrated Services Routers (ISRs). This access point uses a Cisco IOS software image that is separate from the router Cisco IOS software image. It can operate as an autonomous access point that is configured and managed locally, or it can operate as a centrally managed access point using CAPWAP or LWAPP protocol. The AP801 is preloaded with both an autonomous Cisco IOS software release and a recovery image for the unified mode.

When you want to use the AP801 with a controller, you must enable the recovery image for the unified mode on the access point by entering the **service-module wlan-ap 0 bootimage unified** command on the router in privileged EXEC mode.

Note If the **service-module wlan-ap 0 bootimage unified** command does not work, make sure that the software license is current.

After enabling the recovery image, enter the **service-module wlan-ap 0 reload** command on the router to shut down and reboot the access point. After the access point reboots, it discovers the controller, downloads the full CAPWAP or LWAPP software release from the controller, and acts as a lightweight access point.

Note To use the CLI commands mentioned previously, the router must be running Cisco IOS Release 12.4(20)T or later. If you experience any problems, see the "Troubleshooting an Upgrade or Reverting the AP to Autonomous Mode" section in the Integrated Services Router configuration guide at the following URL: http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/admin_ap.html

To support CAPWAP or LWAPP, the router must be activated with at least the Cisco Advanced IP Services IOS license-grade image. A license is required to upgrade to this Cisco IOS image on the router. See the following URL for licensing information:

http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

After the AP801 boots up with the recovery image for the unified mode, it requires an IP address to communicate with the controller and to download its unified image and configuration from the controller. The router can provide DHCP server functionality, the DHCP pool to reach the controller, and setup option 43 for the controller IP address in the DHCP pool configuration. Use the following configuration to perform this task.

```
ip dhcp pool pool_name
    network ip_address subnet_mask
    dns-server ip_address
    default-router ip_address
    option 43 hex controller_ip_address_in_hex
Example:
ip dhcp pool embedded-ap-pool
    network 209.165.200.224 255.255.255.224
    dns-server 209.165.200.225
    default-router 209.165.200.226
    option 43 hex f104.0a0a.0a0f /* single WLC IP address (209.165.201.0) in hex format */
```

The AP801 802.11n radio supports power levels lower than the 802.11n radio in the Cisco Aironet 1250 series access points. The AP801 stores the radio power levels and passes them to the controller when the access point joins the controller. The controller uses the supplied values to limit the user configuration.

The AP801 can be used in FlexConnect mode. See the "Configuring FlexConnect" section on page 12-1 for more information on FlexConnect.

Note For more information about AP801, see the documentation for the Cisco 800 Series ISRs at the following URL: http://www.cisco.com/en/US/products/hw/routers/ps380/tsd_products_support_series_home.html.

Access Point Communication Protocols

In controller software Release 5.2 or later, Cisco lightweight access points use the IETF standard Control and Provisioning of Wireless Access Points (CAPWAP) protocol to communicate between the controller and other lightweight access points on the network. Controller software releases prior to 5.2 use the Lightweight Access Point Protocol (LWAPP) for these communications.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points. CAPWAP is being implemented in controller software Release 5.2 for the following reasons:

- To provide an upgrade path from Cisco products that use LWAPP to next-generation Cisco products that use CAPWAP
- To manage RFID readers and similar devices
- To enable controllers to interoperate with third-party access points in the future

LWAPP-enabled access points are compatible with CAPWAP, and conversion to a CAPWAP controller is seamless. For example, the controller discovery process and the firmware downloading process when using CAPWAP are the same as when using LWAPP. The one exception is for Layer 2 deployments, which are not supported by CAPWAP.

Deployments can combine CAPWAP and LWAPP software on the controllers. The CAPWAP-enabled software allows access points to join either a controller running CAPWAP or LWAPP. The only exception is the Cisco Aironet 1140 Series Access Point, which supports only CAPWAP and therefore joins only controllers running CAPWAP.

Note The Cisco Aironet 1140 series and 3500 series access points associate only with CAPWAP controllers that run WLC versions 7.0 or later.

This section contains the following topics:

Guidelines and Restrictions for Using CAPWAP

- CAPWAP and LWAPP controllers cannot be used in the same mobility group. Therefore, client mobility between CAPWAP and LWAPP controllers is not supported.
- If your firewall is currently configured to allow traffic only from access points using LWAPP, you must change the rules of the firewall to allow traffic from access points using CAPWAP.
- Make sure that the CAPWAP ports are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.
- Any access control lists (ACLs) in your network might need to be modified if CAPWAP uses different ports than LWAPP.

Cisco Wireless LAN Controller Autodiscovery

In a Cisco Unified Network architecture, access points (APs) are lightweight. This means they cannot act independently of a wireless LAN controller (WLC). The access points have to first discover the WLCs and register with them before the AP services the wireless clients.

After the AP has registered to the controller, CAPWAP messages are exchanged and the AP initiates a firmware download from the controller (if there is a version mismatch between the AP and controller). If the onboard firmware of the AP is not the same as the controller, the AP downloads the latest firmware to stay in sync with the controller. The firmware download mechanism utilizes CAPWAP. Then, the controller provisions the AP with the configurations that are specific to the WLANs so that the AP can accept client associations.

Controller Autodiscovery is limited to the Cisco WLAN Solution mobility group subnets defined by the operator.

The Cisco Wireless LAN Controller Autodiscovery:

- Allows operators to search for a single controller by IP address.
- Finds the controller on the network within the specified IP address range.

- Automatically enters the controller information into the Cisco NCS database.

Note Controller Autodiscovery can take a long time in a Class C address range. Because of the large number of addresses in a Class B or Class A range, we recommend that you do not attempt Autodiscovery across Class B or Class A ranges.

As access points associate with a controller, the controller immediately transmits the access point information to Cisco NCS, which automatically adds the access point to the database.

Once the access point information is added to the Cisco NCS database, operators can add the access point to the appropriate spot on a Cisco NCS user interface map.

The Controller Discovery Process

In a CAPWAP environment, a lightweight access point discovers a controller by using CAPWAP discovery mechanisms and then sends it a CAPWAP join request. The controller sends the access point a CAPWAP join response allowing the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

Lightweight access points must be discovered by a controller before they can become an active part of the network. The lightweight access points support the following controller discovery processes:

- Layer 3 CAPWAP or LWAPP discovery—Can occur on different subnets from the access point and uses IP addresses and UDP packets rather than the MAC addresses used by Layer 2 discovery.
- Over-the-air provisioning (OTAP)—This feature is supported by Cisco 4400 series controllers. If this feature is enabled on the controller (in the controller General page), all associated access points transmit wireless CAPWAP or LWAPP neighbor messages, and new access points receive the controller IP address from these messages. This feature is disabled by default and should remain disabled when all access points are installed.
- Locally stored controller IP address discovery—If the access point was previously associated to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the non-volatile memory of an access point. This process of storing controller IP addresses on access points for later deployment is called *priming the access point*.
- DHCP server discovery—This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability.
- DNS discovery—The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.*localdomain* or CISCO-LWAPP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.*localdomain* or CISCO-LWAPP-CONTROLLER.*localdomain*. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

NCS Services

The IT departments within organizations are tasked with meeting increased bandwidth and performance demands, managing a proliferation of new mobile devices, while guaranteeing network access, availability, and regulatory compliance.

Cisco and its partners can work with IT staff to assist with migration to the Cisco Unified Network, making it easier to manage a secure, high-performance, and integrated wired and wireless network that incorporates rich media and diverse mobile devices, including Wi-Fi-enabled phones and tablets.

This section describes the services provided by NCS and contains the following topics:

Cisco Context Aware Service Solution

Context Aware Service (CAS) provides the capability for a Wi-Fi 802.11a/b/g/n network to determine the location of a person or object with an active Wi-Fi device, such as a wireless client or active RFID tag and/or associated data that can be passed by the end point through the wireless infrastructure to an upstream client.

Context Aware Service (CAS) allows a mobility services engine (MSE) to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location and availability from Cisco access points.

The collected contextual information can be viewed in GUI format in the NCS User Interface, the centralized WLAN management platform. NCS is the management system that interfaces with the MSE and serves the user interface (UI) for the services that the MSE provides.

After the MSE installation and initial configurations are complete, the MSE can communicate with multiple Cisco wireless LAN controllers to collect operator-defined contextual information. You can then use the associated NCS to communicate with each MSE to transfer and display selected data.

You can configure the MSE to collect data for clients, switches, rogue access points, rogue clients, mobile stations, and active RFID asset tags.

With Context-Aware Location Services, administrators can determine the location of any 802.11-based device, as well as the specific type or status of each device. Clients (associated, probing, and so on.), rogue access points, rogue clients, and active tags can all be identified and located by the system. See the Context Aware Mobility Solution Deployment Guide for more information.

Note One MSE can be managed by only one NCS, that is, a single MSE cannot be managed by more than one NCS, but a single NCS can manage multiple MSEs. When the number of devices to be managed exceeds the capacity of a single MSE, you need to deploy multiple, independent MSEs.

Cisco Identity Service Engine Solution

The Cisco Identity Services Engine (ISE) is a next-generation identity and policy-based network access platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations.

The Cisco ISE provides a single console where authentication, authorization, posture, guest, and profiling policies can be created and managed. In addition, policy elements can now be reused across all services, reducing the number of tasks and overhead and bringing consistency to the enterprise.

The Cisco ISE gathers information from devices, the infrastructure, and services to enable organizations to build richer contextual policies that can be enforced centrally across the network. The ISE tracks all clients and devices connected to the network, acting as a single source of information for connected user and device identity and location, as well as the health of the endpoint.

The ability to discover, identify, and monitor all IP-enabled endpoint devices gives IT teams complete visibility of both users and "headless" devices on the corporate network.

The Cisco ISE combines AAA, posture, profiling, and guest management capabilities in a single appliance to enforce dynamic access control. The Identity Services Engine can be deployed across the enterprise infrastructure, supporting 802.1x wired, wireless, and VPN networks.

NCS manages the wired and the wireless clients in the network. When Cisco ISE is used as a RADIUS server to authenticate clients, NCS collects additional information about these clients from Cisco ISE and provides all client relevant information to NCS to be visible in a single console.

When posture profiling is enforced in the network, NCS talks to Cisco ISE to get the posture data for the clients and displays it along with other client attributes. When Cisco ISE is used to profile the clients or an endpoint in the network, NCS collects the profiled data to determine what type of client it is, whether it is an iPhone, iPad, an Android device, or any other device.

Cisco ISE is assisting NCS to monitor and troubleshoot client information, and displays all the relevant information for a client in a single console.

Cisco Adaptive Wireless Intrusion Prevention Service

Maintain a constant awareness of your RF environment to minimize legal liability, protect your brand reputation, and assure regulatory compliance.

Cisco Adaptive Wireless Intrusion Prevention System (IPS) offers advanced network security for dedicated monitoring and detection of wireless network anomalies, unauthorized access, and RF attacks. Fully integrated with the Cisco Unified Network, this solution delivers integrated visibility and control across the network, without the need for an overlay solution.

Cisco Adaptive Wireless Intrusion Prevention Service (wIPS) performs rogue access point, rogue client, and ad-hoc connection detection and mitigation, over-the-air wireless hacking and threat detection, security vulnerability monitoring, performance monitoring and self-optimization, network hardening for proactive prevention of threats and complete wireless security management and reporting.

Cisco wIPS is made up of the following components that work together to provide a unified security monitoring solution:

- Mobility services engine (MSE) running wIPS software—Serves as the central point of alarm aggregation for all controllers and their respective wIPS monitor mode access points. Alarm information and forensic files are stored on the mobility services engine for archival purposes.
- A wIPS monitor mode access point—Provides constant channel scanning with attack detection and forensics (packet capture) capabilities.
- Local mode access point—Provides wireless service to clients in addition to time-sliced rogue scanning.
- Wireless LAN Controller—Forwards attack information received from wIPS monitor mode access points to the mobility services engine and distributes configuration parameters to access points.

- Network Control System—Provides a centralized management platform for the administrator to configure the wIPS Service on the mobility services engine, push wIPS configurations to the controller, and configure access points in wIPS monitor mode. NCS is also used to view wIPS alarms, forensics, reporting, and to access the attack encyclopedia.

CHAPTER 2

Getting Started

This chapter describes information on system requirements, setting up and starting the Cisco NCS. The NCS is an application used to configure, manage, and monitor the wired and wireless networks. This chapter contains the following sections:

NCS Delivery Modes

The NCS comes preinstalled on a physical appliance with various performance characteristics. The NCS software runs on either a dedicated NCS appliance or on a VMware server. The NCS software image does not support the installation of any other packages or applications on this dedicated platform. The inherent scalability of the NCS allows you to add appliances to a deployment and increase performance and resiliency.

The NCS is delivered in two modes, the physical appliance and the virtual appliance. This section contains the following topics:

Physical Appliance

The physical appliance is a dual Intel 2.40 GHz Xeon E5620 quad core processor, with 16 GB RAM, and four hard drives running in a RAID level 5 configuration. The physical appliance runs the latest 64-bit Red Hat Linux Operating System.

The physical appliance supports up to 15000 Cisco Aironet lightweight access points, 5000 standalone access points, 5000 switches and 1200 Cisco wireless LAN controllers.

Note To receive the expected results with the NCS, you need a high performance physical appliance with built-in redundancy for hard disks, power supplies and internal cooling fans.

For more information on the physical appliance, see the *Cisco Prime Network Control System Getting Started Guide, Release 1.0*.

Virtual Appliance

The NCS is also offered as a virtual appliance to help support lower level deployments. The NCS can be run on a workstation or a server and access points can be distributed unevenly across controllers.

The NCS virtual appliance software is distributed as an Open Virtualization Archive (OVA) file. There are three recommended levels of the NCS distribution with different resources and numbers of devices supported.

This section contains the following topics:

Note You can deploy the OVA file directly from the vSphere Client; you do not need to extract the archive before performing the deployment.

You can install the NCS virtual appliance using any of the methods for deploying an OVF supported by the VMware environment. Before starting, make sure that the NCS virtual appliance distribution archive is in a location that is accessible to the computer on which you are running the vSphere Client.

Note For more information about setting up your VMware environment, see the VMware vSphere 4.0 documentation.

Virtual Appliance for Large Deployment

- Supports up to 15000 Cisco Aironet lightweight access points, 5000 standalone access points, 5000 switches, and 1200 Cisco wireless LAN controllers.
- 8 Processors at 2.93 GHz or better.
- 16-GB RAM.
- 400 GB minimum free disk space is required on your hard drive.

Note The free disk space listed is a minimum requirement but might be different for your system depending on the number of backups performed.

Virtual Appliance for Medium Deployment

- Supports up to 7500 Cisco Aironet lightweight access points, 2500 standalone access points, 2500 switches, and 600 Cisco wireless LAN controllers.
- 4 Processors at 2.93 GHz or better.
- 12-GB RAM.
- 300 GB minimum free disk space is required on your hard drive.

Virtual Appliance for Small Deployment

- Supports up to 3000 Cisco Aironet lightweight access points, 1000 standalone access points, 1000 switches, and 240 Cisco wireless LAN controllers.
- 2 Processors at 2.93 GHz or better.
- 8-GB RAM.
- 200 GB minimum free disk space is required on your hard drive.

Note For all server levels, AMD processors equivalent to the listed Intel processors are also supported.

Note The free disk space listed is a minimum requirement, but several variables (such as backups) impact the disk space.

Note If you want to use a Cisco UCS Server to deploy a virtual appliance for the NCS, you can use the UCS C-Series or B-Series. Make sure the server you pick matches to the Processor, RAM, and Hard Disk requirements specified in the "Virtual Appliance" section on page 2-2 deployment.

Operating Systems Requirements

The following operating systems are supported:

- Red Hat Linux Enterprise server 5.4 64-bit operating system installations are supported.

  Note You cannot install the NCS on a standalone operating system like Red Hat Linux, as the NCS is shipped as a physical or virtual appliance that comes preinstalled with a secure and hardened operating system.

- Red Hat Linux version support on VMware ESX version 3.0.1 and later with either local storage or SAN over fiber channel.

- The recommended deployments for a virtual appliance are UCS and ESX/ESXi.

Note Individual operating systems running the NCS in VMware must follow the specifications for the size of the NCS that you intend to use.

Client Requirements

The NCS user interface requires Mozilla Firefox 3.6 or later or Internet Explorer 8 with the Chrome plugin releases or Google Chrome 12.0.742.x.

Note We strongly advise that you do not enable third-party browser extensions. In Internet Explorer, you can disable third-party browser extensions by choosing **Tools > Internet Options** and unselecting the **Enable third-party browser extensions** check box on the Advanced tab.

The client running the browser must have a minimum of 1 GB of RAM and a 2-GHz processor. The client device should not be running any CPU or memory-intensive applications.

Note We recommend a minimum screen resolution of 1024 x 768 pixels.

Prerequisites

Before installing the NCS, ensure that you have completed the following:

- Meet the necessary hardware and software requirements for the NCS.
- Check the compatibility matrix for the supported controller, Cisco IOS software releases.
- Update your system with the necessary critical updates and service packs.

  Note See the latest release notes for information on the service packs and patches required for correct operation of the NCS.

- To receive the expected results, you should run no more than 3 concurrent NCS setups for standard server use (4 GB memory and 3 GHz CPU speed) and no more than 5 concurrent NCS setups for high-end server use (8 GB memory and 3 GHz CPU speed).
- Verify that the following ports are open during installation and startup:
  - HTTP: configurable during install (80 by default)
  - HTTPS: configurable during install (443 by default)
  - 1315
  - 1299
  - 6789
  - 8009
  - 8456

- 8005
- 69
- 21
- 162
- 8457

Note Make sure your firewall rules are not restrictive. You can check the current rules on Linux with the built-in iptables -L command.

Reinstalling the NCS on a Physical Appliance

You must have root privileges to install the NCS on a physical appliance.

To reinstall the NCS on a physical appliance, follow these steps:

Step 1 Insert the provided NCS software Image DVD. The system boots up and the following console appears:

```
ISOLINUX 3.11 2005-09-02  Copyright (C) 1994-2005 H. Peter Anvin

           Welcome to Cisco Prime Network Control System

To boot from hard disk, press <Enter>.

Available boot options:

  [1] Network Control System Installation (Keyboard/Monitor)
  [2] Network Control System Installation (Serial Console)
  [3] Recover administrator password. (Keyboard/Monitor)
  [4] Recover administrator password. (Serial Console)
  <Enter> Boot existing OS from Hard Disk.

Enter boot option and press <return>.

boot:
```

Step 2 Select option 1 to reinstall the NCS software image. The system reboots and the configure appliance screen appears.

Step 3 Enter the initial setup parameters and the system reboots again. Remove the DVD and follow the steps to start the NCS server.

Deploying the NCS Virtual Appliance

This section describes how to deploy the NCS virtual appliance from the vSphere Client using the Deploy OVF Wizard or from the command line. (VMware vSphere Client is a Windows application for managing and configuring the vCenter Server.) This section contains the following topics:

- Deploying the NCS Virtual Appliance from the VMware vSphere Client, page 2-6

- Deploying the NCS Virtual Appliance using the Command Line Client, page 2-9

Deploying the NCS Virtual Appliance from the VMware vSphere Client

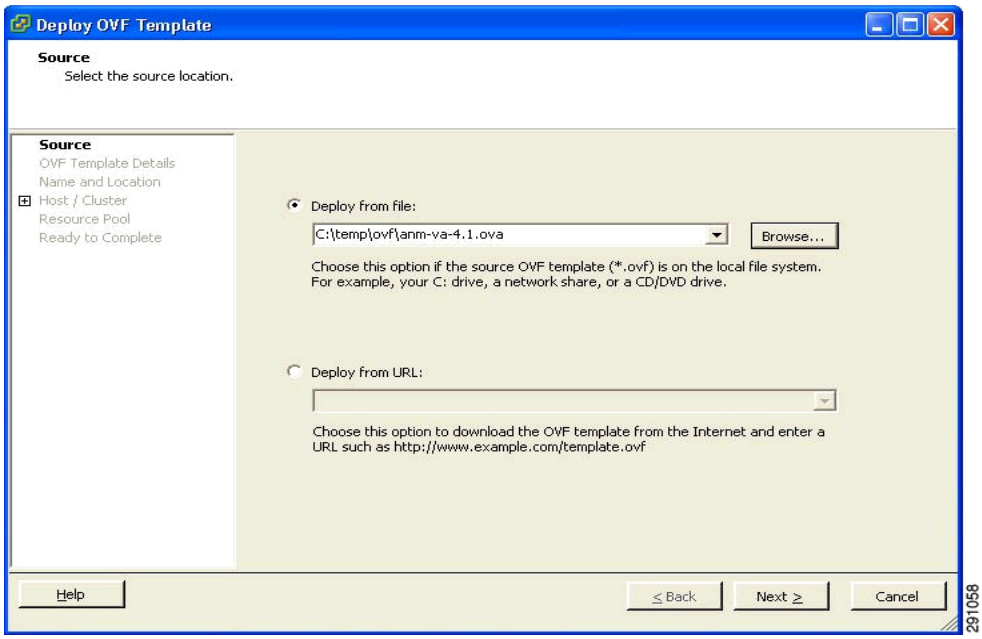
NCS Virtual Image is packaged as an OVF file. An OVF is a collection of items in a single archive. In the vSphere Client, you can use the Deploy OVF Wizard to create a virtual machine, running the NCS virtual appliance application, as described in this section.

Note While the following procedure provides a general guideline for how to deploy the NCS virtual appliance, the exact steps that you need to perform might vary depending on the characteristics of your VMware environment and setup.

To deploy the NCS virtual appliance, follow these steps:

Step 1 From the VMware vSphere Client main menu, choose **File > Deploy OVF Template**. The Deploy OVF Template Source window appears (see Figure 2-1).

Figure 2-1 Deploy OVF Template Window

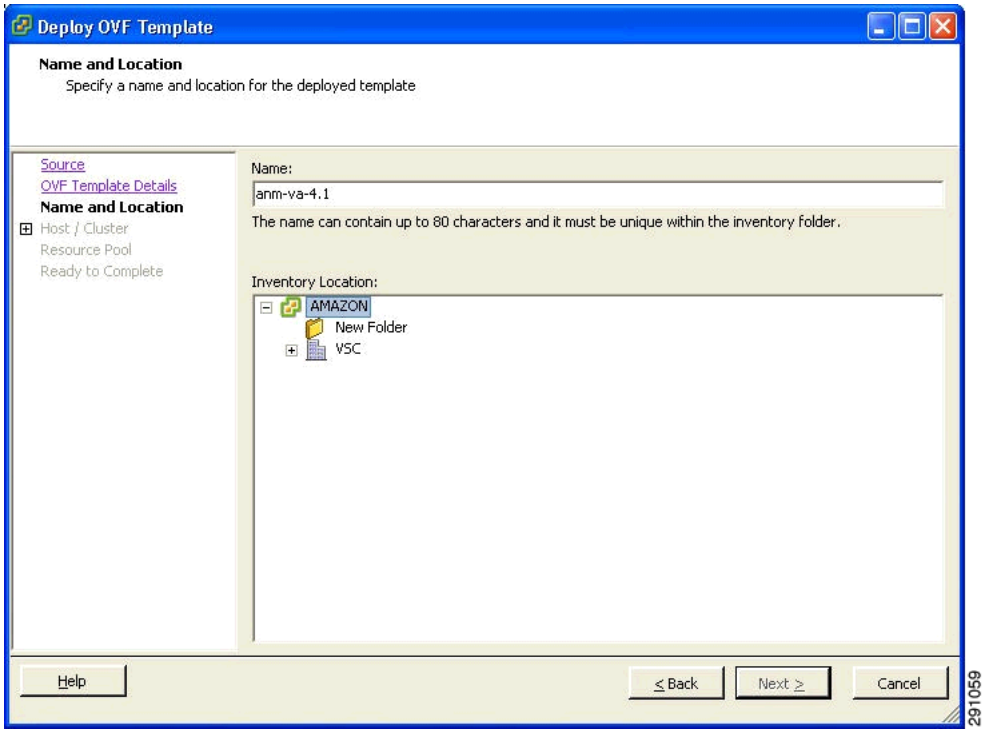


Step 2 Choose **Deploy from file** and choose the OVA file that contains the NCS virtual appliance distribution.

Step 3 Click **Next**. The OVF Template Details window appears. VMware ESX/ESXi reads the OVA attributes. The details include the product you are installing, the size of the OVA file (download size), and the amount of disk space that needs to be available for the virtual machine (size on disk).

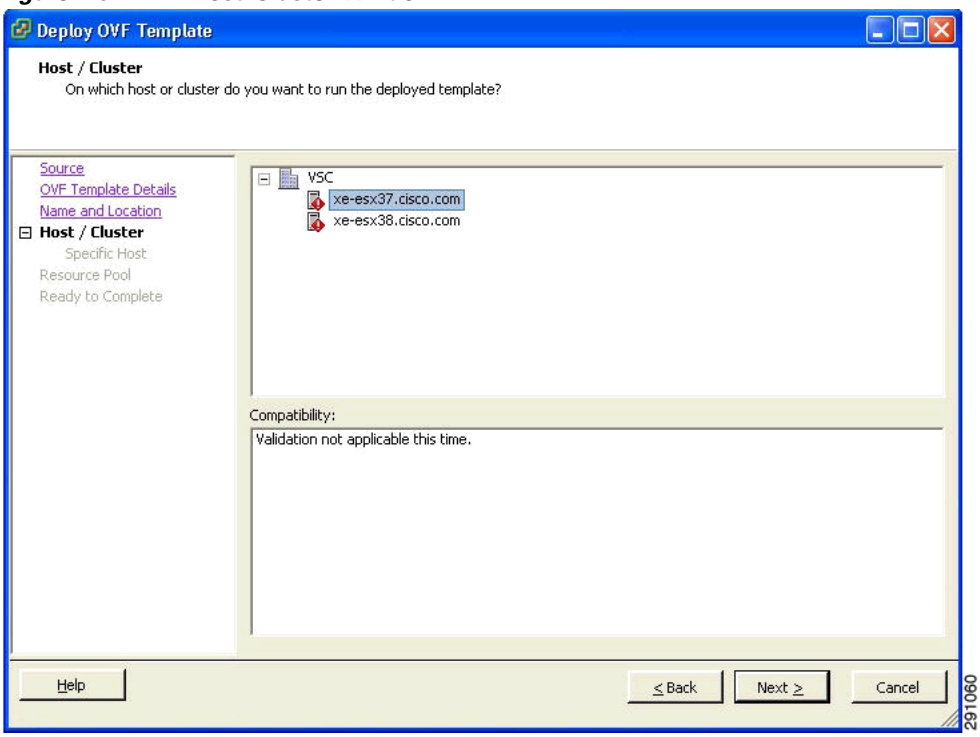
Step 4 Verify the OVF Template details and click **Next**. The Name and Location window appears (see Figure 2-2).

Figure 2-2 Name and Location Window



Step 5 Either keep the default name for the VM to be deployed in the Name text box or provide a new one and click **Next**. This name value is used to identify the new virtual machine in the VMware infrastructure; you should use any name that distinguishes this particular VM in your environment. The Host / Cluster window appears (see Figure 2-3).

Figure 2-3 Host/Cluster Window



Step 6 Choose the destination host or HA cluster on which you want to deploy the NCS VM, and click **Next**. The Resource Pool window appears.

Step 7 If you have more than one resource pool in your target host environment, choose the resource pool to use for the deployment, and click **Next**. The Ready to Complete window appears.

Step 8 Review the settings shown for your deployment and, if needed, click **Back** to modify any of the settings shown.

Step 9 Click **Finish** to complete the deployment. A message notifies you when the installation completes and you can see the NCS virtual appliance in your inventory.

Step 10 Click **Close** to dismiss the Deployment Completed Successfully dialog box.

Configuring the Basic Settings for the NCS Virtual Appliance

You have completed deploying (installing) the NCS virtual appliance on a new virtual machine. A node for the virtual machine now appears in the resource tree in the VMware vSphere Client window. Deploying the OVF template creates a new virtual machine in vCenter with the NCS virtual appliance application and related resources already installed on it. After deployment, you need to configure basic settings for the NCS virtual appliance. To start the NCS setup, follow these steps:

Step 1 In the vSphere Client, click the **NCS virtual appliance** node in the resource tree. The virtual machine node should appear in the Hosts and Clusters tree below the host, cluster, or resource pool to which you deployed the NCS virtual appliance.

Step 2 On the Getting Started tab, click the **Power on the virtual machine** link under Basic Tasks. The Recent Tasks pane at the bottom of the vSphere Client pane indicates the status of the task associated with powering on the virtual machine. After the virtual machine successfully starts, the status column for the task displays Completed.

Step 3 Click the **Console** tab, within the console pane to make the console prompt active for keyboard input.

Now you need to set up the virtual appliance, as described in the "Setting Up the NCS" section on page 2-9.

Deploying the NCS Virtual Appliance using the Command Line Client

This section describes how to deploy the NCS virtual appliance from the command line. As an alternative to using the vSphere Client to deploy the NCS OVA distribution, you can use the VMware OVF Tool, which is a command-line client.

To deploy an OVA with the VMware OVF Tool, use the **ovftool** command, which takes the name of the OVA file to be deployed and the target location as arguments, as in the following example:

```
ovftool NCS-VA-X.X.X-large.ova vi://my.vmware-host.example.com/
```

In this case, the OVA file to be deployed is NCS-VA-X.X.X-large.ova and the target ESX host is my.vmware-host.example.com. For complete documentation on the VMware OVF Tool, see the VMware vSphere 4.0 documentation.

Setting Up the NCS

This section describes how to configure the initial settings of the NCS virtual appliance.

Note These steps need to be performed only once, upon first installation of the NCS virtual appliance.

To configure the basic network and login settings for the NCS virtual appliance system, follow these steps. When the steps are completed, the NCS virtual appliance is accessible over the network.

Note Once you put the NCS Image DVD in the physical appliance for reinstallation, you get the same console prompt. Use the following steps to reinstall the NCS for the physical appliance.

Step 1 At the login prompt, enter the **setup** command.

```
localhost.localdomain login: setup
```

The NCS configuration script starts. The script takes you through the initial configuration steps for the NCS virtual appliance. In the first sequence of steps, you configure network settings.

Step 2 When prompted, enter the following settings:

a. The hostname for the virtual appliance.

b. The IP address for the virtual appliance.

c. The IP default subnet mask for the IP address entered.

d. The IP address of the default gateway for the network environment in which you are creating the virtual machine.

e. The default DNS domain for the target environment.

f. The IP address or hostname of the primary IP nameserver in the network.

g. At the Add/Edit another nameserver prompt, you can enter **y** (yes) to add additional nameservers, if desired. Otherwise, press **Enter** to continue.

h. The NTP server location (or accept the default by pressing **Enter**). At the Add/Edit secondary NTP server prompt, you can enter **y** (yes) to add another NTP server. Otherwise, enter **n** (no) to continue.

Step 3 Enter the username for the user account used to access the NCS system running on the virtual machine. The default username is admin, but you can change this to another username by typing it here.

Step 4 Enter the password for the NCS. The password must be at least eight characters and must include both lowercase and uppercase letters and at least one number. It cannot include the username or default Cisco passwords. After you enter the password, the script verifies the network settings you configured. For example, it attempts to reach the default gateway that you have configured.

After verifying the network settings, the script starts the NCS installation processes. This process can take several minutes, during which there is no screen feedback. When finished, the following banner appears on the screen:

```
=== Initial Setup for Application: NCS ===
```

After this banner appears, the configuration starts with database scripts and reboots the server as shown in the console:

```
Running database cloning script...
logger: invalid option -- l
usage: logger [-is] [-f file] [-p pri] [-t tag] [-u socket] [ message ... ]
Running database creation script...
logger: invalid option -- l
usage: logger [-is] [-f file] [-p pri] [-t tag] [-u socket] [ message ... ]
Setting Timezone, temporary workaround for DB...
Generating configuration...
Rebooting...
```

Note If you are installaing a physical appliance, remove the ISO DVD from the DVD tray.

Step 5 Log in as admin and enter the admin password.

Step 6 Exit the console using the **exit** command.

Starting the NCS Server

This section provides instructions for starting the NCS on either a physical or virtual appliance.

Note You can check the status of the NCS at any time. To do so, follow the instructions in the "Verifying the Status of the NCS" section on page 3-6.

To start the NCS when it is installed on a physical or virtual appliance, follow these steps:

Step 1 Log into the system as administrator.

Step 2 Using the command-line interface, enter the following command:

```
ncs start
```

Logging into the NCS User Interface

To log into the NCS user interface through a web browser, follow these steps:

Step 1 Launch Internet Explorer 7.0 or later or Mozilla Firefox 3.6 or later on a different computer than the one on which you installed and started the NCS.

Note When you use Firefox 3.x to log in and access the NCS for the first time, the Firefox web browser displays a warning stating that the site is untrustable. When Firefox displays this warning, follow the prompts to add a security exception and download the self-signed certificate from the NCS server. After you complete this procedure, Firefox accepts the NCS server as a trusted site both now and during all future login attempts.

Step 2 In the address line of browser, enter https://ncs-ip-address, where ncs-ip-address is the IP address of the server on which you installed and started the NCS. The NCS user interface displays the Login page.

Step 3 Enter your username. The default username is root.

Step 4 Enter the root password you created during setup.

Note If any licensing problems occur, a message appears in an alert box. If you have an evaluation license, the number of days until the license expires is shown. You are also alerted to any expired licenses. You have the option to go directly to the licensing page to address these problems.

Step 5 Click **Login** to log into the NCS. The NCS user interface is now active and available for use. The NCS home page appears. The NCS home page enables you to choose the information that you want to see. You can organize the information in user-defined tabs called dashboards. The default view comes with default dashboards and preselected dashlets for each, and you can arrange them as you like. You can predefine what appears on the home page by choosing the monitoring dashlets that are critical for your network. For example, you might want different monitoring dashlets for a mesh network so that you can create a customized mesh dashboard.

Note If the database or Apache web server does not start, check the launchout.txt file in Linux. You see a generic “failed to start database” or “failed to start the Apache web server” message.

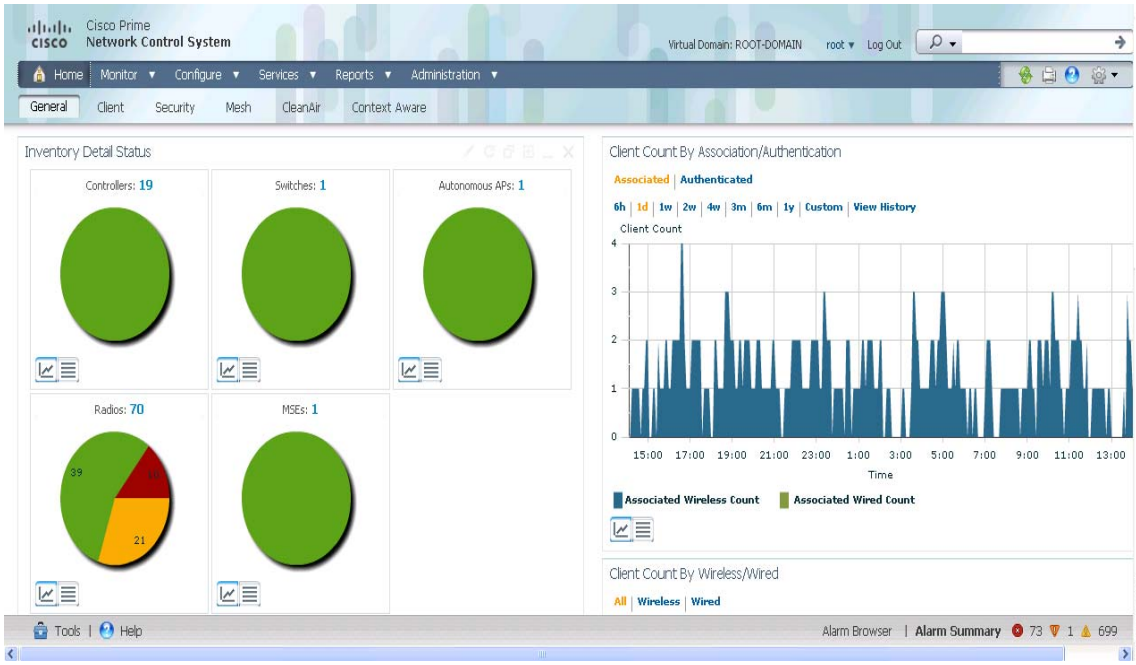
Note When an upgrade occurs, the user-defined tabs arranged by the previous user in the previous version are maintained. Therefore, the latest dashlets might not show. Look at the Edit dashboard link to find what new dashlets are added.

The home page provides a summary of the Cisco Unified Network Solution, including coverage areas, the most recently detected rogue access points, access point operational data, reported coverage holes, and client distribution over time. Figure 2-4 shows a typical NCS home page.

By default, you should see six dashboards in the NCS home page: the General, Client, Security, Mesh, CleanAir, and ContextAware dashboards.

Note When you use the NCS for the first time, the network summary pages show that the Controllers, Coverage Areas, Most Recent Rogue APs, Top 5 APs, and Most Recent Coverage Holes databases are empty. It also shows that no client devices are connected to the system. After you configure the NCS database with one or more controllers, the NCS home page provides updated information.

Figure 2-4 The NCS Home Page



To exit the NCS user interface, close the browser page or click **Log Out** in the upper-right corner of the page. Exiting an NCS user interface session does not shut down the NCS on the server.

When a system administrator stops the NCS server during your NCS session, your session ends, and the web browser displays the message: "The page cannot be displayed." Your session does not reassociate to the NCS when the server restarts. You must restart the NCS session.

Applying the NCS Software License

This section describes how to apply a license to NCS. Before starting, make sure that you have already acquired the license from the Cisco License Center and put it in a location that is accessible by the network from NCS. To add a new NCS license file, follow these steps:

Step 1 In the Administrator menu, choose **License Center > Files > NCS Files** page, and click **Add**.

Step 2 In the Add a License File dialog box, enter or browse to the applicable license file.

Step 3 Once displayed in the License File text box, click **Upload**.

To add a new license, see "Managing Licenses" section on page 15-131.

Understanding the NCS Home Page

The NCS home page:

- Enables the administrator to create and configure Cisco Unified Network Solution coverage area layouts, configure system operating parameters, monitor real-time Cisco Unified Network Solution operations, and perform troubleshooting tasks using an HTTPS web browser page.
- Enables the administrator to create, modify, and delete user accounts; change passwords; assign permissions; and schedule periodic maintenance tasks. The administrator creates new usernames and passwords and assigns them to predefined permissions groups.
- Allows the administrator to perform all necessary network administration tasks from one page. The NCS home page, is the landing page, displaying real-time monitoring and troubleshooting data. The navigation tabs and menus at the top of the page provide point-and-click access to all other administration features.

The NCS user interface provides an integrated network administration console from which you can manage various devices and services. These include wired and wireless devices and clients. The services might include authentication, authorization, profiler, location and mobility services as well as monitoring, troubleshooting, and reporting. All of these devices and services can be managed from a single console called the NCS home page.

This section describes the NCS user interface page and contains the following topics:

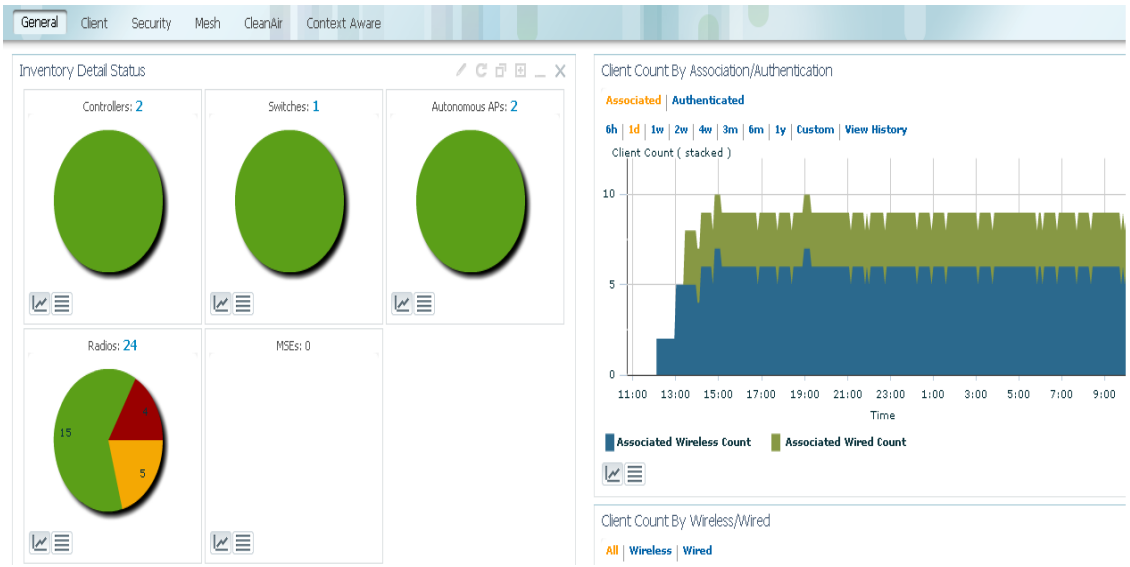
Dashboards

The NCS dashboards consist of dashlets and graphs that provide a visual overview of network health and security. The dashboard elements visually convey complex information in a simplified format. This display allows you to quickly analyze the data and drill down for in-depth information if needed. Dashlets utilize a variety of elements to display data, including pie-charts, sparklines, stack bars, and metric meters.

The fundamental purpose of a dashboard is to provide an at-a-glance view of the most important parts of NCS. A quick scan of the dashboard should let you know if anything needs attention. The dashboard generally provides the status and alerts, monitoring and reporting information. Dashboards contain several dashlets, which are UI containers that display a variety of widgets, such as text, form elements, tables, charts, tabs, and nested content modules.

The dashboard displays the current status which reflects the status and usage of the network, like client distribution. The dashboard also displays the trend which reflects the usage and status over time which is from data collected over time, like client count (see Figure 2-5).

Figure 2-5 Dashboards



Note You must have Adobe Flash Player installed to view the dashlets on the NCS dashboard.

The six NCS dashboards are described in this section. This section contains the following topics:

- General Dashboard, page 2-15
- Client Dashboard, page 2-16
- Security Dashboard, page 2-18
- Mesh Dashboard, page 2-19
- CleanAir Dashboard, page 2-19
- Context Aware Dashboard, page 2-21

You can customize the predefined set of dashlets depending on your network management needs. You can organize the information in user-defined dashboards. The default view comes with default dashboards and pre-selected dashlets for each.

Note

- The label "*Edited*" next to the dashlet heading indicates that the dashlet has been customized. If you reset to the default settings, the Edited label is cleared. Hover your mouse cursor over the label see the edited information.
- When an upgrade occurs, the arrangement of dashlets in a previous version is maintained. Because of this, dashlets or features added in a new release are not displayed. Click the **Manage Dashboards** link to discover new dashlets.
- The horizontal and vertical scrollbars are visible if you zoom the dashlets. Reset the zoom level back to zero, or no zoom for viewing the dashlets without the scrollbars.

General Dashboard

Table 2-1 lists the factory default dashlets for the General dashboard.

Table 2-1 General Dashboard

Dashlet	Description
Inventory Detail Status	Displays the following: • Controllers—Lists the number of controllers that are managed in NCS. Graphically depicts reachable and unreachable controllers. • Switches—Lists the number of switches managed in NCS. Graphically depicts reachable and unreachable switches. • Radios—Lists the number of radios managed in NCS. Graphically depicts the number of radios in out-of-service (critical), minor, and ok conditions. This dashlet reflects ONLY the greatest radio alarm status, that is, if the radio has a minor alarm, and a critical alarm, then the radio status shows as critical. • Autonomous APs—Lists the number of Autonomous APs managed in NCS. Graphically depicts reachable and unreachable Autonomous APs. • MSEs—Lists the number of MSEs that are managed in NCS. Graphically depicts reachable and unreachable servers. Look at the installation log to verify that nothing went wrong while manually adding the servers to NCS. (The trace for MSEs must be turned on.) **Note** Clicking the corresponding sections of the chart takes you to the item list view of the inventory.
Device Uptime	Displays the devices based on the device up time.
Coverage Area	Displays access points, radios, and client details for each coverage area.

Table 2-1 General Dashboard (continued)

Dashlet	Description
Client Count by Association/Authentication	Displays the total number of clients by Association and authentication in NCS over the selected period of time. • Associated client—All clients are connected regardless of whether it is authenticated or not. • Authenticated client—All clients are connected through an RADIUS or TACACS server. **Note** Client count includes autonomous clients.
Client Count by Wireless/Wired	Displays the total number of clients by Wired and Wireless in NCS over the selected period of time. **Note** Client count includes autonomous clients.
Top 5 Devices by Memory Utilization	Displays the Top 5 devices based on memory utilization.
Recent Coverage Holes	Displays the five most recent coverage alarms.

Client Dashboard

Table 2-2 lists the factory default dashlets for the Client dashboard.

Table 2-2 Client Dashboard

Dashlet	Description
Client Troubleshooting	Allows you to troubleshoot a client by entering a client MAC address, then clicking **Troubleshoot**.
Client Distribution	Displays the distribution of clients by protocol, EAP type, and authentication and the total current client count. • 802.3 represents wired clients • 802.11 represents wireless clients **Note** Clicking the corresponding sections of the chart takes you the item list view of the clients and users.
Client Alarms and Events Summary	Displays a summary of client alarms and events.
Client Traffic	Displays the trend of both upstream and downstream client traffic in a given time period.

Table 2-2 Client Dashboard (continued)

Dashlet	Description
Client Traffic by IP Address Type	Displays the client traffic for the following types of IP addresses: • IPv4 Upstream • IPv4 Downstream • IPv6 Upstream • IPv6 Downstream • Dual Stack (IPv4/IPv6) Upstream • Dual Stack (IPv4/IPv6) Downstream
Wired Client Speed Distribution	Displays the wired client speeds and the client count for each speed.
Top 5 SSIDs by Client Count	Displays the top 5 SSID client counts.
Top 5 Switches by Client Count	Displays the 5 switches that have the most clients, as well as the number of clients associated to the switch.
Client Posture Status	Displays the client posture status and the number of clients in each of the following status categories: • Compliant • Non-compliant • Unknown • Pending • Not Applicable • Error
IP Address Type Distribution	Displays the count of clients for the following types of IP addresses: • IPv4 Upstream • IPv4 Downstream • IPv6 Upstream • IPv6 Downstream • Dual Stack (IPv4/IPv6) Upstream • Dual Stack (IPv4/IPv6) Downstream

Security Dashboard

Table 2-3 lists the factory default dashlets for the Security dashboard.

Table 2-3 Security Dashboard

Dashlet	Description
Security Index	Indicates the security of the NCS managed network. The security index is calculated by assigning priority to the various security configurations and displaying them in visual form.
Malicious Rogue APs	Displays malicious rogue access points for the past hour, past 24 hours, and total active.
Unclassified Rogue APs	Displays unclassified rogue access points for the past hour, past 24 hours, and total active.
Friendly Rogue APs	Displays friendly rogue access points for the past hour, past 24 hours, and total active.
Adhoc Rogues	Displays ad hoc rogues for the past hour, past 24 hours, and total active.
CleanAir Security	Displays Cleanair security events for past hour, 24 hours, and total active.
Attacks Detected	Displays wIPS and signature attacks for the past hour, past 24 hours, and total active.
Cisco Wired IPS Events	Displays Wired IPS events for the past hour, past 24 hours, and total active.
AP Threats/Attacks	Displays threats or attacks to access points for the past hour, past 24 hours, and total active.
MFP Attacks	Displays MFP attacks for the past hour, past 24 hours, and total active.
Client Security Events	Displays the client security events for the past hour, past 24 hours and total active.

Note The Rogue alarm, which is set as informational, cannot be seen in the Security dashboard.

Mesh Dashboard

Table 2-4 lists the factory default dashlets for the Mesh dashboard.

Table 2-4 Mesh Dashboard

Dashlet	Description
Most Recent Mesh Alarms	Displays the five most recent mesh alarms. Click the number in parentheses to access the Alarms page.
Mesh Worst SNR Links	Displays the worst signal-to-noise ratio (SNR) links. Data includes the Parent AP Name, the Child AP Name, and the Link SNR.
Mesh Worst Node Hop Count	Displays the worst node hop counts. Data includes the AP Name, the Hop Count, and the Parent AP Name.
Mesh Worst Packet Error Rate	Displays the worst packet error rates. Data includes the Parent AP Name, the Child AP Name, and the Packet Error Rate.

CleanAir Dashboard

Table 2-5 lists the factory default dashlets for the Mesh dashboard.

Table 2-5 CleanAir Dashboard

Dashlet	Description
802.11a/n Avg Air Quality	Provides a line chart representing the average air quality for the entire network over a set period of time. Displays the average air quality on the 802.11 a/n band. Data includes time and the average air quality.
802.11b/g/n Avg Air Quality	Provides a line chart representing the average air quality for the entire network over a set period of time. Displays the average air quality on the 802.11 b/g/n band. Data includes time and the average air quality.
802.11a/n Min Air Quality	Provides a line chart representing the minimum air quality for the entire network over a set period of time. Displays the minimum air quality on the 802.11 a/n band. Data includes time and the minimum air quality.
802.11b/g/n Min Air Quality	Provides a line chart representing the minimum air quality for the entire network over a set period of time. Displays the minimum air quality on the 802.11 b/g/n band. Data includes time and minimum air quality.

Table 2-5 CleanAir Dashboard (continued)

Dashlet	Description
Worst 802.11a/n Interferers	Provides a list of active interferers with the worst severity level for the 802.11 a/n band. The graph displays the top ten worst interferers that are currently active. Data includes InterfererID, Type, Status, Severity, Affected Channels, Duty Cycle(%), Discovered, Last Updated, and Floor.
Worst 802.11b/g/n Interferers	Provides a list of active interferers with the worst severity level for 802.11 b/g/n band. The graph displays the top ten worst interferers that are currently active. Data includes InterfererID, Type, Status, Severity, Affected Channels, Duty Cycle(%), Discovered, Last Updated, and Floor.
802.11a/n Interferer Count	Provides a line chart representing the total number of interferers on all channels over the selected period of time. Displays the number of devices interfering in the 802.11 a/n band. Data includes time and interferer count. **Note** The air quality is calculated for all controllers in your network that have CleanAir-enabled access points. The report includes aggregated air quality data across your network.
802.11b/g/n Interferer Count	Provides a line chart representing the total number of interferers on all channels over the selected period of time. Displays the number of devices interfering in the 802.11 b/g/n band. Data includes time and interferer count. **Note** The information in the worst interferer and interferer count charts is collected from the mobility services engines (MSE). If MSEs are not available, this chart does not show any results.
Recent-Security risk Interferers	Provides a list of active interferers with the worst severity level for each band. Displays the recent security risk interferers on your wireless network. Data includes Type, Severity, Affected Channels, Last Detected, Detected AP. **Note** This chart includes information for the interferers for which security alarms are enabled. You can also view the data presented on this dashlet in different formats.

Context Aware Dashboard

Table 2-6 lists the factory default dashlets for the Context Aware dashboard.

Table 2-6 Context Aware Dashboard

Dashboard	Description
MSE Historical Element Count	Displays the historical trend of tags, clients, rogue APs, rogue clients, interferers, wired clients, and guest client counts in a given period of time. **Note** The MSE Historical Count information is presented in a time-based graph. For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed. See the "Time-Based Graphs" section on page 6-71 for more information.
Rogue Elements detected by CAS	Displays the indices of the Rogue APs and Rogue Clients in percentage. It also provides a count of the number of Rogue APs and Rogue Clients detected by each MSE within an hour, 24 hours as well as more than 24 hours. Rogue AP Index is defined as the percentage of total active tracked elements that are detected as Rogue APs across all the MSEs on NCS. Rogue Client Index is defined as the percentage of total active tracked elements that are detected as Rogue Clients across all the MSEs on NCS.
Location Assisted Client Troubleshooting	You can troubleshoot clients using this option with location assistance. You can provide either a MAC Address, Username, or IP Address as the criteria for troubleshooting. **Note** Username, IP address, and partial MAC address-based troubleshooting is supported only on MSEs with Version 7.0.200.0 and later. For more information about Location Assisted Client Troubleshooting, see the "Context Aware Dashboard" section on page 2-21.

Table 2-6 Context Aware Dashboard (continued)

Dashboard	Description
MSE Tracking Counts	Represents the tracked and not-tracked count of each of the element types. The element type includes tags, rogue APs, rogue clients, interferers, wired clients, wireless clients, and guest clients.
Top 5 MSEs	Lists the top five MSEs based on the percentage of license utilization. It also provides count for each element type for each MSE. **Note** If you have installed NCS license but you have not added any MSE to NCS then the Context-Aware dashboard is empty. However a message is displayed with a link to add an MSE. In the dashlet, click the count link to get a detailed report. Use the icons in a dashlet to switch between chart and grid view. Use the Enlarge Chart icon to view the grid or chart in full screen.

Icons

The icons on the dashlets and within the General, Client, Security, Mesh, CleanAir, and Context Aware dashboards have the following functions listed in Table 2-7.

Table 2-7 Icon Representation

Icon	Description
	The Dashlet Options icon enables you to customize and filter the data by using variables and search options. For example, you can search the client count trends for SSIDs, floor areas, controllers, specific autonomous APs, and so on.
	The Refresh Dashlet icon enables you to automatically refresh the dashboard so that it reflects the current network status.
	The Detach Dashlet icon enables you to detach the dashlet.
	The Maximize Dashlet icon enables you to maximize the dashlet so that it is visible in full view.
	The collapse Dashlet icon enables you to minimize the dashlet so that the dashlet is not visible.

Table 2-7 Icon Representation

Icon	Description
	The View in Chart icon enables you to view the dashlet in chart rather than table form.
	The View in Grid icon enables you to view the dashlet in a table rather than chart form.

Menu Bar

The primary form of navigation used in NCS is the menu located at the top of the NCS page. Administrators can monitor and perform various tasks from this menu. This menu is an easy-access, pop-up menu that provides quick access to the submenus that are associated with the primary menu. Hover your mouse cursor over any menu title to access the associated menu. Clicking the menu title takes you directly to the feature page. The following illustration is an example of the primary NCS menu (see Figure 2-6).

Figure 2-6 NCS Primary Global Menu

This section describes the menus and contains the following topics:

- Monitor Menu, page 2-23
- Configure Menu, page 2-24
- Services Menu, page 2-25
- Reports Menu, page 2-25
- Administration Menu, page 2-25

When you hover your mouse cursor over any of the five menu titles, a drop-down menu appears.

Monitor Menu

The Monitor menu provides you with a top-level description of your network devices. You can monitor your network, maps, Google Earth maps, network devices (controllers, switches, access points, clients, tags, chokepoints, Wi-Fi TDOA receivers), RRM, alarms, and events.

The following submenu options are available from the Monitor menu:

- Monitoring Devices
  - Monitoring Controllers
  - Monitoring Switches
  - Monitoring Access Points
  - Monitoring RFID Tags

  - Monitoring Chokepoints
  - Monitoring Interferers
  - Monitoring WiFi TDOA Receivers
- Monitoring Radio Resource Management (RRM)
- Monitoring Clients and Users
- Monitoring Alarms and Events
  - Monitoring Alarms
  - Monitoring Events
- Monitoring Maps
  - Monitoring Maps
  - Monitoring Google Earth Maps

Configure Menu

The Configure menu enables you to configure templates, controllers, access points, switches, chokepoints, Wi-Fi TDOA receivers, config groups, auto provisioning, scheduled configuration tasks, profiles, ACS view servers, and TFTP servers on your network.

The following submenu options are available from the Configure drop-down menu:

- Configuring Devices
  - Configuring Controllers
  - Configuring Switches
  - Configuring Unknown Devices
  - Configuring Access Points
  - Configuring Chokepoints
  - Configuring Spectrum Experts
  - Configuring Wi-Fi TDOA Receivers
- Configuring Scheduled Configuration Tasks
- Establishing Logging Options
- Configuring wIPS Profiles
- Configuring Templates
  - Accessing the Controller Template Launch Pad
  - Configuring Lightweight Access Point Templates
  - Configuring Autonomous Access Point Templates
  - Configuring Switch Location Configuration Templates
  - Configuring Autonomous AP Migration Templates
- Configuring Controller Config Groups
- Configuring Servers
  - Configuring ACS View Servers
  - Configuring TFTP or FTP Servers

Services Menu

The Services menu enables you to manage mobility services including mobility services engines and Identity Service Engines.

The following submenu options are available from the Services drop-down menu:

- Mobility Services
  - Viewing Current Mobility Services
  - Synchronizing Services
  - Viewing Synchronization History
  - Viewing the Notifications Summary for Mobility Services
- Identity Services

Reports Menu

The Reports menu provides the following submenu options:

- Report Launch Pad
- Managing Scheduled Run Results
- Managing Saved Report Templates

Administration Menu

The Administration menu enables you to schedule tasks like making a backup, checking a device status, auditing your network, synchronizing the MSE, and so on. It also contains Logging to enable various logging modules and specify restart requirements. For user administration such as changing passwords, establishing groups, setting application security settings, and so on, choose AAA. From the Administration Menu, you can also access the licensing information, set user preferences, and establish high availability (a secondary backup device running NCS).

The following submenu options are available from the Administration drop-down menu:

- Performing Background Tasks
- Configuring a Virtual Domain
- Configuring Administrative Settings
- Managing Licenses
- Viewing Appliance Details
- Configuring AAA
- Establishing Logging Options
- Configuring High Availability
- Managing Licenses

Global Toolbar

The Global toolbar is always available at the bottom of the NCS page, providing instantaneous access to the tools, NCS online Help system, and a summary of alarm notifications. Hover your mouse cursor over the Help icon to access the available online Help (see Figure 2-7).

Hover your mouse cursor over the Alarms Browser to display the summarized Alarms page, with a list of recent system alarms and the ability to filter for alarms of a specific nature. You can also drill down for detailed information on individual alarms. For more information on Alarms, see the "Alarm Summary" section on page 2-27.

Figure 2-7 Global Toolbar

This section contains the following topics:

Tools

The Tools menu provides access to the Voice Audit, Configuration Audit, and Migration Analysis features of NCS.

The following submenu options are available from the Tools drop-down menu:

- Voice Audit
- Location Accuracy Tools
- Config Audit
- Migration Analysis
- TAC Case Attachment

Help

The Help menu allows you to access online help, learning modules, submit feedback, and to verify the current version of NCS. The Help icon is located in the bottom left corner of the Global Toolbar in the NCS page. The Help provides quick access to the comprehensive online Help for NCS.

The following submenu options are available from the Help drop-down menu:

- Online Help—Enables you to view online Help. The online Help is context sensitive and opens documentation for the NCS window that you currently have open.
- Learning Modules—Allows you to access short video clips of certain NCS features. To learn more about Cisco NCS features and functionality, go to Cisco.com to watch multimedia presentations about NCS configuration workflow, monitoring, troubleshooting, and more. Over future releases, more overview and technical presentations will be added to enhance your learning.
- MSE Installation Guide—Provides links to the MSE installation section.
- Submit Feedback—Allows you to access a page where you can enter feedback about the NCS.

- Help Us Improve Cisco Products—Allows you to enable and provide permission to automatic collect data about how you and your organization use your Cisco wireless products, this data is useful to improve product performance and usability. The data is automatically collected and sent to Cisco in encrypted form. The data might contain information about your organization and it is not be shared or used outside of Cisco.

Note To get the automated feedback enabled, you must configure your Mail Server Configuration by choosing **Administration > Settings > Mail Server Configuration**.

- About Cisco NCS—Allows you to verify the version of NCS that you are running. It provides the version, hostname, feature, AP limit, and type.

To verify the version of NCS, choose **About Cisco NCS**. The following information is displayed:

- Product Name
- Version Number
- Host Name
- Feature
- AP Limit
- License Type
- Copyright statement

Alarm Summary

When NCS receives an alarm message from a controller, it displays an alarm indicator at the bottom of the NCS page (see Figure 2-8). Alarms indicate the current fault or state of an element that needs attention, and they are usually generated by one or more events. The alarm can be cleared but the event remains. The Critical (red), Major (orange) and Minor (yellow) alarms appear in the alarm dashboard, left to right.

Note The Administration > Settings > Alarms page has a Hide Acknowledged Alarms check box that you must unselect it if you want acknowledged alarms to appear in the NCS and alarms lists page. By default, acknowledged alarms are not shown.

Figure 2-8 NCS Alarm Summary

Note Alarm counts are refreshed every 15 seconds.

Command Buttons

The NCS user interface uses a number of command buttons throughout its pages. The most common command buttons are as follows:

- Apply—Applies the selected information

- Delete—Deletes the selected information
- Cancel—Cancels new information entered on the current page and returns to the previous page
- Save—Saves the current settings
- Audit—Discovers the present status of this access point
- Place AP—Audits the configuration of the selected entity by flagging the differences between NCS database device configurations

Main Data Page

The main data page is determined by the required parameter information. Active areas on the data pages include the following:

- Text boxes into which data might be entered
- Drop-down lists from which one of several options might be chosen
- Check boxes allow you to choose one or more items from the displayed list
- Radio buttons allow you to turn a parameter on or off
- Hyperlinks take you to other pages in the NCS user interface

Input text boxes are black text on a white background. When data is entered or selected, it is not sent to the controller, but it is saved in the text box until you click **Go**.

Administrative Elements

The following provides information regarding the current NCS user:

- User—Indicates the username for the current NCS user. Click the User link to change the user password. See the "Changing Password" section on page 15-87 for more information.
- Virtual Domain—Indicates the current virtual domain for this NCS user. See the "Configuring a Virtual Domain" section on page 15-41 for more information.

Note To switch domain names, click the blue inverted triangle icon located at the right of the virtual domain name to open the switch to another Virtual Domain page. Select the **new virtual domain** radio button, and click **Save**. Your privileges are changed accordingly.

Icon	Description
	Click to access the NCS online help. **Note** The online Help provides information applicable to your current NCS version.
	Click to update the data in the current NCS version.

Icon	Description
	Click to access a print-friendly version of the current NCS. **Note** Click **Print** to print the current NCS version or **Exit Print View** to return to the previous page.
	Click to edit the dashboard or to add a new dashboard in NCS.

Customizing the NCS Home Page

NCS home page dashlets contain a default, predefined list of dashlets that you can customize. The following customizations are possible in the NCS home page:

- Drag-and-drop dashlets
- Add or delete dashboards
- Reordering dashboards
- Renaming dashlets and dashboards
- Customize layout

Note You can add or delete dashlets by selecting from the predefined list.

You can customize the home page with time-based or non-time-based interactive graphs which you can display in grid or chart format (by clicking the appropriate icon). These graphs refresh automatically within a predetermined time based on the default polling cycles of dependent tasks, or you can click the Refresh dashlet icon to get the most current status. You can click the Enlarge Chart icon to enlarge the graph in a separate page.

This section contains the following topics:

- Editing the NCS Home Page, page 2-29
- Adding Dashlets, page 2-30
- Adding a New Dashboard, page 2-32

Editing the NCS Home Page

To customize the NCS home page dashlets, follow these steps:

Step 1 In the NCS home page, click  . The drop-down menu appears.

Step 2 Click **Add Dashlet** to view a list of the available dashlets. Add the desired dashlet by clicking **Add** in the right column. The dashlet is added to the appropriate dashboard.

Step 3 Click **Apply**.

Adding Dashlets

Table 2-8 lists the default dashlet options you can add in your NCS home page.

Table 2-8 Default Dashlets

Dashlet	Description
AP Join Taken Time	Displays the access point name and the amount of time (in days, minutes, and seconds) that it took for the access point to join.
AP Threats/Attacks	Displays various types of access point threats and attacks and indicates how many of each type have occurred.
AP Uptime	Displays each access point name and amount of time it has been associated.
Ad hoc Rogues	Displays ad hoc rogues for the previous hour, previous 24 hours, and total active.
Cisco Wired IPS Events	Displays wired IPS events for the previous hour, previous 24 hours, and total active.
Client	Displays the five most recent client alarms with client association failures, client authentication failures, client WEP key decryption errors, client WPA MIC errors, and client exclusions.
Client Authentication Type	Displays the number of clients for each authentication type.
Client Count	Displays the trend of associated and authenticated client counts in a given period of time.
Client Distribution	Displays how clients are distributed by protocol, EAP type, and authentication type.
Client EAP Type Distribution	Displays the count based on the EAP type.
Client Protocol Distribution	Displays the current client count distribution by protocols.
Client Security Events	Displays client security events within the previous 24 hours including excluded client events, WEP decrypt errors, WPA MIC errors, shunned clients, and IPsec failures.
Client Traffic	Displays the trend of client traffic in a given time period.
Client Troubleshooting	Allows you to enter a MAC address of a client and retrieve information for diagnosing the client in the network.
Clients Detected by Context Aware Service	Displays the client count detected by the context aware service within the previous 15 minutes.
Controller CPU Utilization (%)	Displays the average, maximum, and minimum CPU usage.
Controller Memory Utilization	Displays the average, maximum, and minimum memory usage as a percentage for the controllers.

Table 2-8 Default Dashlets (continued)

Dashlet	Description
Coverage Areas	Displays the list coverage areas and details about each coverage area.
Friendly Rogue APs	Displays friendly rogue access points for the previous hour, previous 24 hours, and total active.
Guest Users Count	Displays Guest client count over a specified time.
Inventory Detail Status	Displays the Chart summarizing the status for the following device types. - Controllers - Switches - Autonomous APs - Radios - MSEs
Inventory Status	Displays the total number of client controllers and the number of unreachable controllers.
LWAPP Uptime	Displays the access point name and the amount of its uptime in days, minutes, and seconds.
Latest 5 Logged in Guest Users	Displays the most recent guest users to log in.
Mesh AP by Hop Count	Displays the APs based on hop count.
Mesh AP Queue Based on QoS	Displays the APs based on QoS.
Mesh Parent Changing AP	Displays the worst Mesh APs based on changing parents.
Mesh Top Over Subscribed AP	Displays the considered over subscribed APs.
Mesh Worst Node Hop Count2-28	Displays the Worst AP node hop counts from the root AP.
Mesh Worst Packet Error Rate	Displays the worst Mesh AP links based on the packet error rates of the links.
Mesh Worst SNR Link	Displays the worst Mesh AP links based on the SNR values of the links.
Most Recent AP Alarms	Displays the five most recent access point alarms. Click the number in parentheses to open the Alarms page which shows all alarms.
Most Recent Client Alarms	Displays the most recent client alarms.
Most Recent Mesh Alarms	Displays the most recent mesh alarms
Most Recent Security Alarms	Displays the five most recent security alarms. Click the number in parentheses to open the Alarms page.
Recent 5 Guest User Accounts	Displays the most recent guest user accounts created or modified.

Table 2-8 Default Dashlets (continued)

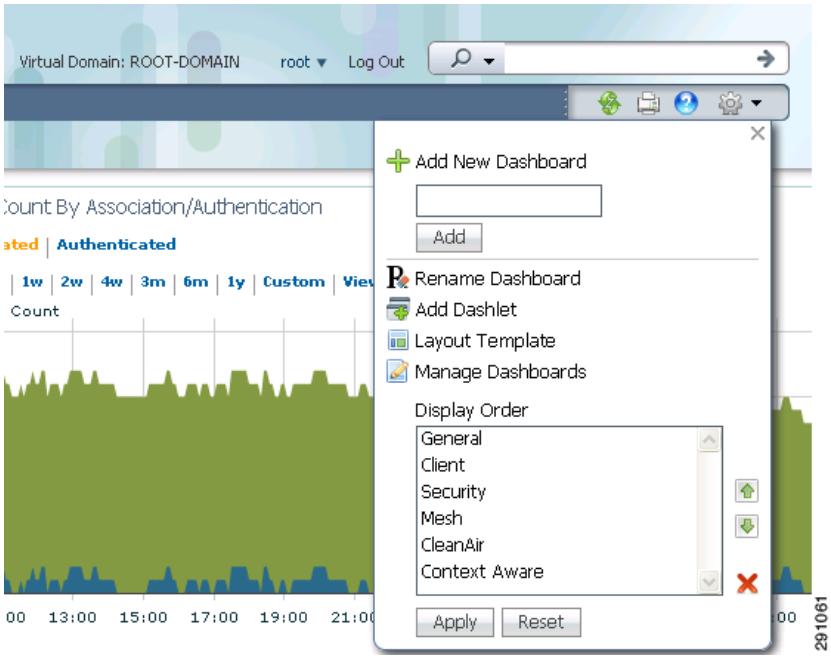
Dashlet	Description
Recent Alarms	Displays the five most recent alarms by default. Click the number in parentheses to open the Alarms page.
Recent Coverage Holes	Displays the recent coverage hole alarms listed by access point.
Recent Malicious Rogue AP Alarms	Displays the recent malicious rogue AP alarms.
Recent Rogue Alarms	Displays the five most recent rogue alarms. Click the number in parentheses to open the Alarms page which shows the alarms.
Security Index	Displays the security index score for the wireless network. The security index is calculated as part of the 'Configuration Sync' background task.
Top APs by Client Count	Displays the Top APs by client count.
Unclassified Rogue APs	Displays unclassified rogue access points for the previous hour, previous 24 hours, and total active.

Adding a New Dashboard

To create a new dashboard, follow these steps:

Step 1 Click ⚙ ▾ in NCS home page. The drop-down menu appears (see Figure 2-9).

Figure 2-9 Edit Dashboard



Step 2 Enter the name of the new dashboard you are creating, and click **Add**. The dashboard name you just added appears in the Display Order list.

Note Add is the only function that does not require a Save operation after its operation. If you click **X**, Move Up, or Move Down, you must click **Apply** for the changes to be applied.

Step 3 You can add dashlets to the new dashboard. For more information see the "Adding Dashlets" section on page 2-30.

Note If you want to return to the restored factory defaults as shown in Figure 2-8, click **Reset** to reset to factory defaults.

Using the Search Feature

The enhanced NCS Search feature (see Figure 2-10) provides easy access to advanced search options and saved searches. You can access the search options from any page within NCS making it easy to search for a device or SSID (Service Set IDentifier).

Figure 2-10 NCS Search Feature

The following searches are possible using NCS:

- Quick Search, page 2-33
- Advanced Search, page 2-34
- Saved Searches, page 2-46

Quick Search

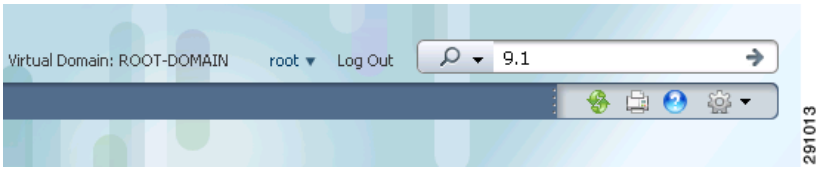
For a quick search, you can enter a partial or complete IP address, MAC address, name, or SSID for clients, alarms, access points, controllers, maps, tags, or rogue clients (see Figure 2-10).

Note You can also enter a username if you are searching for a client.

To quickly search for a device, follow these steps:

Step 1 Enter the complete or partial IP address, device name, SSID, or MAC address of the device in the Search text box (see Figure 2-11).

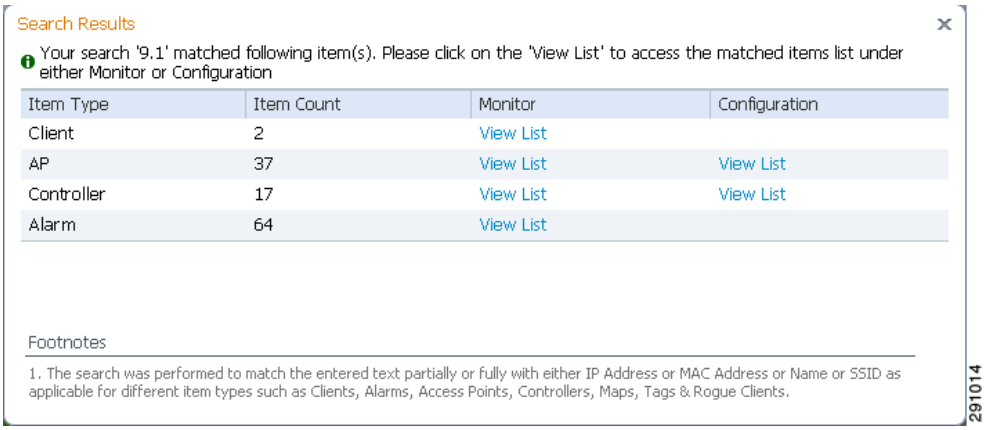
Figure 2-11 Quick Search with Partial IP Address



Step 2 Click **Search** to display all devices that match the Quick Search parameter.

The search results display the matching item type, the number of items that match your search parameter, and links to the list of matching results (see Figure 2-12). Click **View List** to view the matching devices in the Monitor or Configuration pages.

Figure 2-12 Quick Search Results Advanced Search



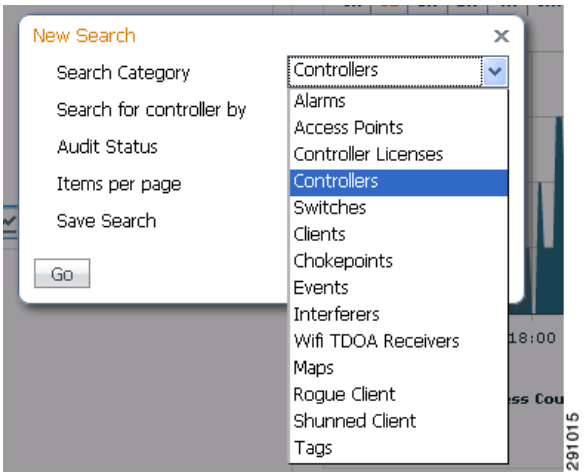
Advanced Search

To perform a more specific search for a device in NCS, follow these steps:

Step 1 Click **Advanced Search** located in the top right corner of NCS (see Figure 2-10).

Step 2 In the New Search dialog, choose a category from the Search Category drop-down list (see Figure 2-13).

Figure 2-13 Search Category Drop-Down List



Note Click each of the following categories for more information.

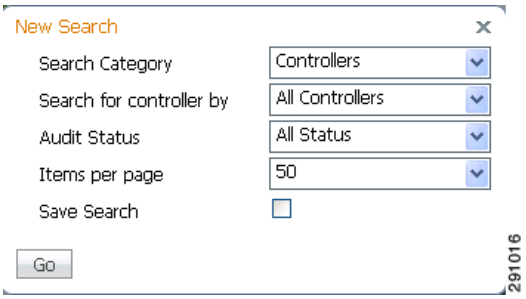
Search categories include the following:

- Alarms
- Access Points
- Controller Licenses
- Controllers
- Switches
- Clients
- Chokepoints
- Events
- Interferers
- Wi-Fi TDOA Receivers
- Maps
- Rogue Client
- Shunned Client
- Tags

Step 3 Select all applicable filters or parameters for your search (see Figure 2-14).

Note Search parameters change depending on the selected category. The following pre-defined search filters have been added in Release 6.0: Associated Clients, Authenticated Clients, Excluded Clients, Probing Clients, All Clients, New Clients detected in last 24 hours, unauthenticated clients, 2.4 GHz clients, and 5 GHz clients.

Figure 2-14 New Search Fields



Step 4 Choose the number of items to display on the results page.

Step 5 To save this search, select the **Save Search** check box and enter a name for the search in the text box.

Step 6 When all filters and parameters are set, click **Go**.

Searching Alarms

You can configure the following parameters when performing an advanced search for alarms (see Table 2-9).

Table 2-9 Search Alarms Fields

Field	Options
Severity	Choose **All Severities**, **Critical**, **Major**, **Minor**, **Warning**, or **Clear**.
Alarm Category	Choose **All Types**, **Access Points**, **Controller**, **Switches**, **Coverage Hole**, **Config Audit**, **Mobility Service**, **Context Aware Notifications**, **Interference**, **Mesh Links**, **Rogue AP**, **Adhoc Rogue**, **Security**, **NCS**, or **Performance**.
Condition	Use the drop-down list to choose a condition. Also, you can enter a condition by typing it in this drop-down list. **Note** If you have selected an alarm category, this drop-down list would contain the conditions available in that category.
Time Period	Choose a time increment from Any Time to Last 7 days. The default is Any Time.

Table 2-9 Search Alarms Fields (continued)

Field	Options
Acknowledged State	Select this check box to search for alarms with an Acknowledged or Unacknowledged state. If this check box is not selected, the acknowledged state is not taken into search criteria consideration.
Assigned State	Select this check box to search for alarms with an Assigned or Unassigned state or by Owner Name. If this check box is not selected, the assigned state is not part of the search criteria. **Note** If you choose Assigned State > Owner Name, type the owner name in the available text box.

Note You can decide what information appears on the alarm search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Searching Access Points

You can configure the following parameters when performing an advanced search for access points (see Table 2-10).

Table 2-10 Search Access Points Fields

Field	Options
Search By	Choose **All APs**, **Base Radio MAC**, **Ethernet MAC**, **AP Name**, **IP Address**, **Controller Name**, **Controller IP**, **All Unassociated APs**, **Floor Area**, **Outdoor Area**, **Unassigned APs**, or **Alarms**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select Floor Area, you also must identify its campus and building. Or, if you select Alarms, you can search for access points based on the severity of the alarm.
AP Type	Choose **All Types**, **LWAPP**, or **Autonomous**.
AP Mode	Choose **All Modes**, **Local, Monitor**, **FlexConnect**, **Rogue Detector**, **Sniffer**, **Bridge**, or **SE-Connect**.

Table 2-10 Search Access Points Fields (continued)

Field	Options
Radio Type	Choose **All Radios**, **802.11a**, or **802.11b/g**.
802.11n Support	Select this check box to search for access points with 802.11n support.
OfficeExtend AP Enabled	Select this check box to search for OfficeExtend access points.
CleanAir Support	Select this check box to search for access points which support CleanAir.
CleanAir Enabled	Select this check box to search for access points which support CleanAir and which are enabled.
Items per page	Configure the number of records to be displayed in the search results page.

Note You can decide what information appears on the access points search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Searching Controller Licenses

You can configure the following parameters when performing an advanced search for controller licenses (see Table 2-11).

Table 2-11 Search Controller Licenses Fields

Field	Options
Controller Name	Type the controller name associated with the license search.
Feature Name	Choose **All**, **Plus**, or **Base** depending on the license tier.
Type	Choose **All**, **Demo**, **Extension**, **Grace Period**, or **Permanent**.
% Used or Greater	Choose the percentage of the license use from this drop-down list. The percentages range from 0 to 100.
Items per page	Configure the number of records to be displayed in the search results page.

See the "Managing Licenses" section on page 15-131 for more information on licenses and the License Center.

Searching Controllers

You can configure the following parameters when performing an advanced search for controllers (see Table 2-12).

Table 2-12 Search Controllers Fields

Field	Options
Search for controller by	Choose **All Controllers**, **IP Address**, or **Controller Name**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Enter Controller IP Address	This text box appears only if you choose IP Address from the Search for controller by drop-down list.
Enter Controller Name	This text box appears only if you choose Controller Name from the Search for controller by drop-down list.
Audit Status	Choose one of the following from the drop-down list: • **All Status** • **Mismatch**—Config differences were found between the NCS and controller during the last audit. • **Identical**—No config differences were found during the last audit. • **Not Available**—Audit status is unavailable.
Items per page	Configure the number of records to be displayed in the search results page.

Note You can decide what information appears on the controllers search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Searching Switches

You can configure the following parameters when performing an advanced search for switches (see Table 2-13).

Table 2-13 Search Switches Fields

Field	Options
Search for Switches by	Choose **All Switches**, **IP Address**, or **Switch Name**. You can use wildcards (*). For example, if you select IP Address and enter **172***, NCS returns all switches that begin with IP address 172.
Items per page	Configure the number of records to be displayed in the search results page.

You can decide what information displays on the client search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Searching Clients

You can configure the following parameters when performing an advanced search for clients (see Table 2-14).

Table 2-14 Search Clients Fields

Field	Options
Media Type	Choose **All**, **Wireless Clients**, or **Wired Clients**.
Wireless Type	Choose **All**, **Lightweight** or **Autonomous Clients** if you chose Wireless Clients from the Media Type list.
Search By	Choose **All Clients**, **All Excluded Clients**, **All Wired Clients**, **All Logged in Guests**, **IP Address**, **User Name**, **MAC Address**, **Asset Name**, **Asset Category**, **Asset Group**, **AP Name**, **Controller Name**, **Controller IP**, **MSE IP**, **Floor Area**, **Outdoor Area**, **Switch Name**, or **Switch Type**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select IP address, you must enter the specific IP address for this search.
Clients Detected By	Choose **NCS** or **MSEs**. Clients detected by the NCS—Clients stored in NCS databases. Clients detected by MSE—Clients located by Context Aware service in the MSE directly communicating with the controllers.
Client States	Choose **All States**, **Idle**, **Authenticated**, **Associated**, **Probing**, or **Excluded**.
Posture Status	Choose **All**, **Unknown**, **Passed**, **Failed** if you want to know if the devices are clean or not.

Table 2-14 Search Clients Fields (continued)

Field	Options
Restrict By Radio Band	Select the check box to indicate a specific radio band. Choose **5 GHz** or **2.4 GHz** from the drop-down list.
Restrict By Protocol	Select the check box to indicate a specific protocol. Choose **802.11a**, **802.11b**, **802.11g**, **802.11n**, or **Mobile** from the drop-down list.
SSID	Select the check box and choose the applicable SSID from the drop-down list.
Profile	Select the check box to list all of the clients associated to the selected profile. **Note** Once the check box is selected, choose the applicable profile from the drop-down list.
CCX Compatible	Select the check box to search for clients that are compatible with Cisco Client Extensions. **Note** Once the check box is selected, choose the applicable version, **All Versions**, or **Not Supported** from the drop-down list.
E2E Compatible	Select the check box to search for clients that are end–to–end compatible. **Note** Once the check box is selected, choose the applicable version, **All Versions**, or **Not Supported** from the drop-down list.
NAC State	Select the check box to search for clients identified by a certain Network Admission Control (NAC) state. **Note** Once the check box is selected, choose the applicable state from the drop-down list: **Quarantine**, **Access**, **Invalid**, and **Not Applicable**.
Include Disassociated	Select this check box to include clients that are no longer on the network but for which the NCS has historical records.
Items per page	Configure the number of records to be displayed in the search results page.

Note You can decide what information appears on the client search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Searching Chokepoints

You can configure the following parameters when performing an advanced search for chokepoints (see Table 2-15).

Table 2-15 Search Chokepoint Fields

Field	Options
Search By	Choose **MAC Address** or **Chokepoint Name**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select MAC address, you must enter the specific MAC address for this search.

Searching Events

You can configure the following parameters when performing an advanced search for events (see Table 2-16).

Table 2-16 Search Events Fields

Field	Options
Severity	Choose **All Severities**, **Critical**, **Major**, **Minor**, **Warning**, **Clear**, or **Info. Color coded**.
Event Category	Choose **All Types**, **Access Points**, **Controller**, **Security**, **Coverage Hole, Rogue AP**, **Adhoc Rogue**, **Interference**, **Mesh Links**, **Client**, **Mobility Service**, **Location Notifications**, **Pre Coverage Hole**, or **NCS**.
Condition	Use the drop-down list to choose a condition. Also, you can enter a condition by typing it in this drop-down list. **Note** If you selected an event category, this drop-down list contains the conditions available in that category.
Search All Events	Configure the number of records to be displayed in the search results page.

See the "Monitoring Rogue Alarm Events" section on page 5-113 for more information on events.

Searching Interferers

You can configure the following parameters when performing an advanced search for interferers detected by access points (see Table 2-17).

Table 2-17 Search SE-Detected Interferers Fields

Field	Options
Search By	Choose **All Interferers**, **Interferer ID**, **Interferer Category**, **Interferer Type**, **Affected Channel**, **Affected AP**, **Severity**, **Power**, or **Duty Cycle**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Detected By	Choose **All Spectrum Experts** or a specific spectrum expert from the drop-down list.
Detected within the last	Choose the time range for the interferer detections. The times range from 5 minutes to 24 hours to All History.
Interferer Status	From this drop-down list, choose **All**, **Active**, or **Inactive**.
Restrict by Radio Bands/Channels	Configure the search by radio bands or channels.
Items per page	Configure the number of records to be displayed in the search results page.

You can decide what information appears on the SE-detected interferers search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Searching AP-Detected Interferers

You can configure the following parameters when performing an advanced search for interferers detected by access points (see Table 2-18).

Table 2-18 Search AP-Detected Interferers Fields

Field	Options
Search By	Choose **All Interferers**, **Interferer ID**, **Interferer Type**, **Affected Channel**, **Severity**, **Duty Cycle**, or **Location**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Detected within the last	Choose the time range for the interferer detections. The times range from 5 minutes to 24 hours to All History.
Active Interferers Only	Select the check box to only include active interferers in your search.

Note You can decide what information appears on the AP-detected interferers search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Searching Wi-Fi TDOA Receivers

You can configure the following parameters when performing an advanced search for Wi-Fi TDOA receivers (see Table 2-19).

Table 2-19 Search Wi-Fi TDOA Receivers Fields

Field	Options
Search By	Choose **MAC Address** or **Wi-Fi TDOA Receivers Name**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

Searching Maps

You can configure the following parameters when performing an advanced search for maps (see Table 2-20).

Table 2-20 Search Map Fields

Field	Options
Search for	Choose **All Maps**, **Campuses**, **Buildings**, **Floor Areas**, or **Outdoor Areas**.
Map Name	Search by Map Name. Enter map name in the text box.
Items per page	Configure the number of records to be displayed in the search results page.

Note You can decide what information appears on the maps search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

See the "Information About Maps" section on page 4-2 for more information on maps.

Searching Rogue Clients

You can configure the following parameters when performing an advanced search for rogue clients (see Table 2-21).

Table 2-21 Search Rogue Client Fields

Field	Options
Search for clients by	Choose **All Rogue Clients**, **MAC Address**, **Controller**, **MSE**, **Floor Area**, or **Outdoor Area**.

Table 2-21 Search Rogue Client Fields (continued)

Field	Options
Search In	Choose **MSEs** or **NCS Controllers**.
Status	Select the check box and choose **Alert**, **Contained**, or **Threat** from the drop-down list to include status in the search criteria.

See the "Rogue Access Points, Ad hoc Events, and Clients" section on page 3-9 for more information on rogue clients.

Searching Shunned Clients

Note When a Cisco IPS sensor on the wired network detects a suspicious or threatening client, it alerts the controller to shun this client.

You can configure the following parameters when performing an advanced search for shunned clients (see Table 2-22).

Table 2-22 Search Shunned Client Fields

Field	Options
Search By	Choose **All Shunned Clients**, **Controller**, or **IP Address**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

Searching Tags

You can configure the following parameters when performing an advanced search for tags (see Table 2-23).

Table 2-23 Search Tags Fields

Field	Options
Search for tags by	Choose **All Tags**, **Asset Name**, **Asset Category**, **Asset Group**, **MAC Address**, **Controller**, **MSE**, **Floor Area**, or **Outdoor Area**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Search In	Choose **MSEs** or **NCS Controllers**.

Table 2-23 Search Tags Fields (continued)

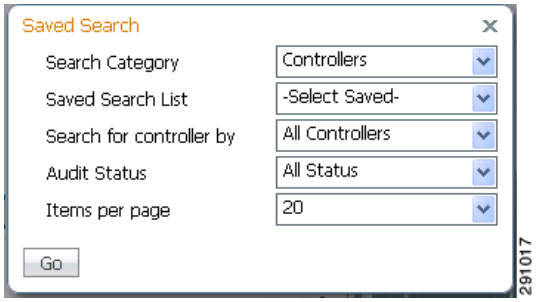
Field	Options
Last detected within	Choose a time increment from 5 minutes to 24 hours. The default is 15 minutes.
Tag Vendor	Select the check box and choose Aeroscout, G2, PanGo, or WhereNet.
Telemetry Tags only	Select the Telemetry Tags only check box to search tags accordingly.
Items per page	Configure the number of records to be displayed in the search results page.

Saved Searches

The Saved Search feature enables you to access and run any previously saved search (see Figure 2-15).

Note When saving a search, you must assign a unique name to the search. Saved searches apply only to the current partition.

Figure 2-15 Saved Search Page



To access and run a saved search, follow these steps:

Step 1 Click **Saved Search**.

Step 2 Choose a category from the Search Category drop-down list.

Step 3 Choose a saved search from the Saved Search List drop-down list.

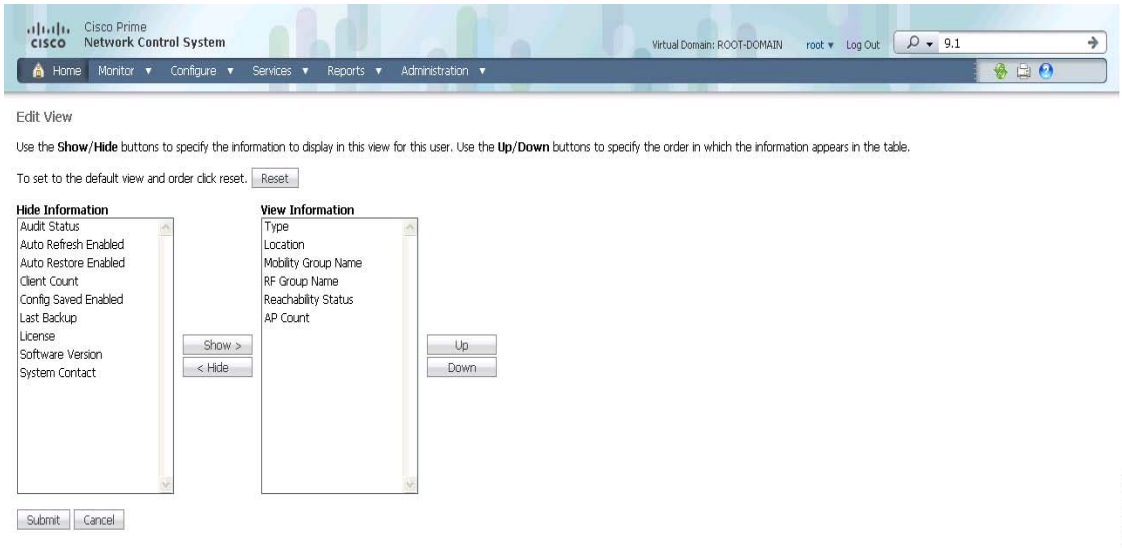
Step 4 If necessary, change the current parameters for the saved search.

Step 5 Click **Go**.

Configuring the Search Results Display (Edit View)

The Edit View page (see Figure 2-16) enables you to choose which columns appear on the Search Results page.

Figure 2-16 Edit View Page



Column names appear in one of the following lists:

- Hide Information—Lists columns that do not appear in the table. The Hide button points to this list.
- View Information—Lists columns that do appear in the table. The Show button points to this list.

To display a column in a table, click it in the Hide Information list, then click **Show**. To remove a column from a table, click it in the View Information list, then click **Hide**. You can select more than one column by holding down the shift or control key.

To change the position of a column in the View Information list, click it, then click **Up** or **Down**. The higher a column is in the list, the farther left it appears in the table.

Command Buttons

The following command buttons appear in the Edit View page:

- Reset—Sets the table to the default display.
- Show—Moves the highlighted columns from the Hide Information list to the View Information list.
- Hide—Moves the highlighted columns from the View Information list to the Hide Information list.
- Up—Moves the highlighted columns upward in the list (further to the left in the table).
- Down—Moves the highlighted columns downward in the list (further to the right in the table).
- Submit—Saves the changes to the table columns and returns to the previous page.
- Cancel—Undoes the changes to the table columns and returns to the previous page.

CHAPTER 3

Configuring Security Solutions

This chapter describes the security solutions for wireless LANs. It contains the following sections:

Cisco Unified Wireless Network Solution Security

The Cisco Unified Wireless Network Solution bundles potentially complicated Layer 1, Layer 2, and Layer 3 802.11 access point security components into a simple policy manager that customizes system-wide security policies on a per wireless LAN basis. It provides simple, unified, and systematic security management tools.

One of the challenges to wireless LAN deployment in the enterprise is Wired Equivalent Privacy (WEP) encryption, which is a weak standalone encryption method. A more recent problem is the availability of low-cost access points that can be connected to the enterprise network and used to mount man-in-the-middle and denial of service attacks. Also, the complexity of add-on security solutions has prevented many IT managers from embracing the benefits of the latest advances in wireless LAN security.

This section contains the following topics:

Layer 1 Solutions

The Cisco Unified Wireless Network Solution operating system security solution ensures that all clients gain access within an operator-set number of attempts. Should a client fail to gain access within that limit, it is automatically excluded (blocked from access) until the operator-set timer expires. The operating system can also disable SSID broadcasts on a per wireless LAN basis.

Layer 2 Solutions

If a higher level of security and encryption is required, the network administrator can also implement industry-standard security solutions such as 802.1X dynamic keys with Extensible Authentication Protocol (EAP) or Wi-Fi Protected Access (WPA) dynamic keys. The Cisco Unified Wireless Network Solution WPA implementation includes Advanced Encryption Standard (AES), Temporal Key Integrity Protocol + message integrity code checksum (TKIP + Michael MIC) dynamic keys, or static WEP keys. Disabling is also used to automatically block Layer 2 access after an operator-set number of failed authentication attempts.

Regardless of the wireless security solution selected, all Layer 2 wired communications between controllers and access points are secured by passing data through Lightweight Access Point Protocol (LWAPP) tunnels.

Layer 3 Solutions

The WEP problem can be further solved using industry-standard Layer 3 security solutions such as Virtual Private Networks (VPNs).

The Cisco Unified Wireless Network Solution supports local and RADIUS Media Access Control (MAC) filtering. This filtering is best suited to smaller client groups with a known list of 802.11 access card MAC addresses. The Cisco Unified Wireless Network Solution also supports local and RADIUS user/password authentication. This authentication is best suited to small to medium client groups.

Single Point of Configuration Policy Manager Solutions

When the Cisco Unified Wireless Network Solution is equipped with Cisco NCS, you can configure system-wide security policies on a per wireless LAN basis. Small office, home office (SOHO) access points force you to individually configure security policies on each access point or use a third-party appliance to configure security policies across multiple access points. Because the Cisco Unified Wireless Network Solution security policies can be applied across the whole system from the NCS, errors can be eliminated, and the overall effort is greatly reduced.

Rogue Access Point Solutions

This section describes security solutions for rogue access points and contains the following topics:

Rogue Access Point Challenges

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain text, other denial of service, or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as passwords and usernames. The hacker can then transmit a series of clear-to-send (CTS) frames, which mimics an access point informing a particular wireless LAN client adapter to transmit and instructing all others to wait. This scenario results in legitimate clients being unable to access the wireless LAN resources. Thus, wireless LAN service providers have a strong interest in banning rogue access points from the air space.

The operating system security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access points, automatically discover rogue access points, and locate them as described in the "Tagging and Containing Rogue Access Points" section on page 3-3.

Tagging and Containing Rogue Access Points

When the Cisco Unified Wireless Network Solution is monitored using the NCS, the NCS generates the flags as rogue access point traps and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the access points closest to each rogue access point. The next step is to mark them as Known or Acknowledged rogue access points (no further action), Alert rogue access points (watch for and notify when active), or Contained rogue access points (have between one and four access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

Securing Your Network Against Rogue Access Points

You can secure your network against any rogue access points and disallow access point attacks for those access points not defined in the MAC filter list.

To set up MAC filtering, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address for which you want to enter MAC filters.

Step 3 Choose **Security > AAA > MAC Filtering** from the left sidebar menu. The MAC Filtering page appears (see Figure 3-1).

Figure 3-1 MAC Filtering Page

The RADIUS compatibility mode, MAC delimiter, MAC address, profile name, interface, and description appears.

Step 4 If you want to set the same configuration across multiple devices, you can choose **Add MAC Filter** from the Select a command drop-down list, and click **Go**. If a template exists, you can apply it. If you need to create a template, you can click the URL to get redirected to the template creation page.

Note The ability to join a controller without specification within a MAC filter list is only supported on mesh access points.

Step 5 To make changes to the profile name, interface, or description, click a specific MAC address in the MAC Address column.

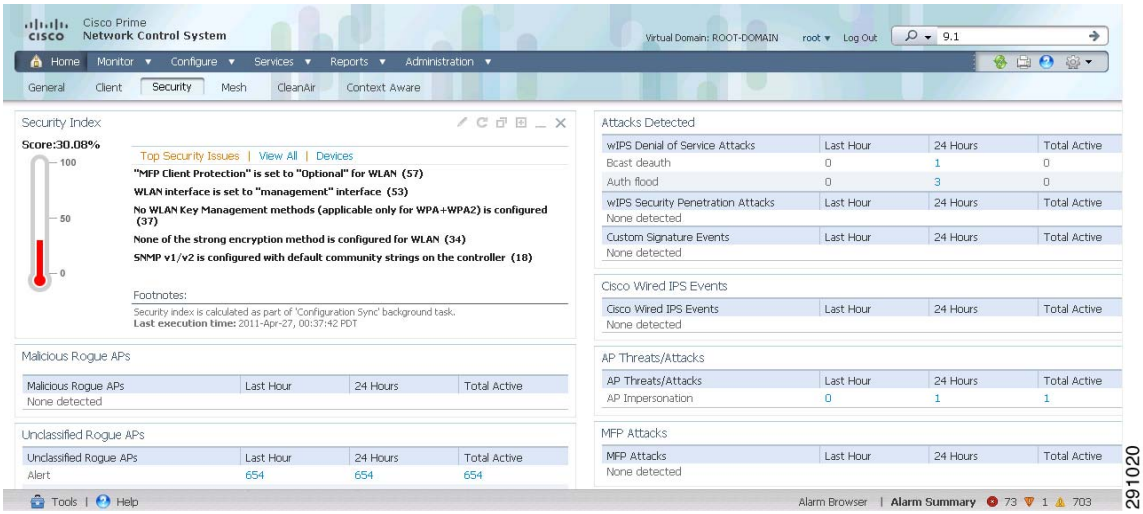
Interpreting the Security Dashboard

Because unauthorized rogue access points are inexpensive and readily available, employees sometimes plug them into existing LANs and build ad hoc wireless networks without IT department knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. Even more alarming, wireless users frequently publish insecure access point locations, increasing the odds of having the enterprise security breached.

Rather than having a person with a scanner manually detect rogue access points, the Cisco Unified Wireless Network Solution automatically collects information on rogue access points detected by its managed access points (by MAC and IP address) and allows the system operator to locate, tag, and contain them. It can also be used to discourage rogue access point clients by sending them deauthenticate and disassociate messages from one to four access points.

For a summary of existing events and the security state of the network, click the **Security** dashboard from the NCS home page. Figure 3-2 shows the security dashboard and different dashlets.

Figure 3-2 Security Dashboard



This section describes the Security dashboard, dashlets and contains the following topics:

- Security Index, page 3-5
- Malicious Rogue Access Points, page 3-6
- Adhoc Rogues, page 3-6
- CleanAir Security, page 3-7
- Unclassified Rogue Access Points, page 3-7
- Friendly Rogue Access Points, page 3-8
- Access Point Threats or Attacks, page 3-8
- MFP Attacks, page 3-9
- Attacks Detected, page 3-9

You can customize the order of information you want the Security dashboard to display. You can move the dashlets to change the order. Use the Edit Dashlet icon to customize the information displayed in the dashlet. You can change the dashlet title, enable refresh, and set the refresh time interval using the Edit Dashlet icons.

Security Index

The Security Index dashlet indicates the security of the NCS managed network, and it is calculated as part of daily background tasks. It is calculated by assigning weight to the various security configurations and displaying it in visual form. The combined weighting can vary from 0 to 100 where 0 signifies the least secured and 100 is the maximum secured. The weighting comes from the lowest scoring controller and the lowest scoring Location Server/Mobility Service Engine related security configurations that are maintained within the NCS itself. The Security Index of the NCS managed network is equal to the lowest scoring controller plus the lowest scoring Location Service/Mobility Service Engine.

The security thermometer color range is represented as follows:

- Above or equal to 80 - Green
- Below 80 but greater than or equal to 60 - Yellow
- Below 60 - Red

Note Guest WLANs are excluded from the WLANs. A WLAN that has web authentication or web passthrough enabled is identified as a guest WLAN.

The security index of the latest release is the benchmark for the required security configurations. For example, if AES encryption was not present in an earlier version of code, the index is reduced by the number associated with the AES encryption security configuration. Likewise, if new security configurations are introduced, the weighting would be altered.

Note The configurations stored in the NCS might not be the latest with the ones in the controllers unless the Refresh from Controller command is run from the NCS. You can run Security Index calculations from the Configuration Sync task to get the latest configuration data from all the controllers. See the "Performing a Configuration Sync" section on page 15-10 for steps on enabling the security index.

Malicious Rogue Access Points

This dashlet provides information on rogue access points that are classified as *Malicious*. Table 3-1 describes the various parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

Note Malicious access points are detected as untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification.

Table 3-1 Malicious Rogue AP Details

Field	Description
Alert	Indicates the number of rogues in an alert state. **Note** An access point is moved to Alert if it is not on the neighbor list or part of the user-configured Friendly AP list.
Contained	Indicates the number of contained rogues.
Threat	Indicates the number of threat rogues.
Contained Pending	Indicates the number of contained rogues pending. **Note** Contained Pending indicates that the containment action is delayed due to unavailable resources.

Adhoc Rogues

The Adhoc Rogues dashlet displays the rogues that have occurred in the last hour, last 24 hours, and the total active. Table 3-2 describes the various parameters. If you click the number in any of these columns, a page with further information appears.

Note The Adhoc Rogue state is displayed as *Alert* when first scanned by the controller or as *Pending* when operating system identification is underway.

Table 3-2 Ad hoc Rogues

Field	Description
Alert	Indicates the number of ad hoc rogues in an alert state. **Note** An access point is moved to Alert if it is not on the neighbor list or part of the user-configured Friendly AP list.
Contained	Indicates the number of contained rogues.
Threat	Indicates the number of threat rogues.
Contained Pending	Indicates the number of contained rogues pending. **Note** Contained pending indicates that the containment action is delayed due to unavailable resources.

CleanAir Security

This dashlet provides information on CleanAir security and provides information about the security-risk devices active during the last hour, 24 hours, and Total Active security-risk devices on the wireless network.

The following information is displayed:

- Severity
- Failure Source
- Owner
- Date/Time
- Message
- Acknowledged

To learn more about the security-risk interferers, see the "Monitoring CleanAir Security Alarms" section on page 5-144.

Unclassified Rogue Access Points

Table 3-3 describes the unclassified rogue access point parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

Note An unclassified rogue access point refers to a rogue access point that is not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list.

Table 3-3 Unclassified Rogue Access Points

Field	Description
Alert	Number of unclassified rogues in alert state. Rogue access point radios appear as *Alert* when first scanned by the controller or as *Pending* when operating system identification is underway.
Contained	Number of contained unclassified rogues.
Contained Pending	Number of contained unclassified rogues pending.

Friendly Rogue Access Points

This dashlet provides information on rogue access points that are classified as *friendly*. Table 3-4 describes the various parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

Note Friendly rogue access points are known, acknowledged, or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.

Table 3-4 Friendly Rogue AP Details

Field	Description
Alert	Indicates the number of rogues in an alert state. **Note** An access point is moved to Alert if it is not on the neighbor list or part of the user-configured Friendly AP list.
Internal	Indicates the number of internal access points. **Note** Internal indicates that the detected access point is inside the network and has been manually configured as Friendly - Internal.
External	Indicates the number of external access points. **Note** External indicates that the detected access point is outside of the network and has been manually configured as Friendly - External.

Access Point Threats or Attacks

Table 3-5 describes the AP Threats or Attacks parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

Table 3-5 AP Threats/Attacks

Field	Description
Fake Attacks	Number of fake attacks.
AP Missing	Number of missing access points.
AP Impersonation	Number of access point impersonations.
AP Invalid SSID	Number of invalid access point SSIDs.
AP Invalid Preamble	Number of invalid access point preambles.
AP Invalid Encryption	Number of invalid access point encryption.
AP Invalid Radio Policy	Number of invalid access point radio policies.
Denial of Service (NAV related)	Number of Denial of Service (NAV related) request.
AP Detected Duplicate IP	Number of detected duplicate access point IPs.

MFP Attacks

A value is provided for Infrastructure and client MFP attacks in the last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

Attacks Detected

A value is provided for wIPS Denial of Service and wIPS Security Penetration attacks and custom signature attacks for the past hour, past 24 hours, and total active. If you click an underline number in any of the time period categories, a page with further information appears.

Recent Rogue AP Alarms

A value is provided for the five most recent rogue alarms. Click the number in parentheses to access the Alarms page. Then click an item under MAC address to view alarm details.

Recent Adhoc Rogue Alarm

Displays the five most recent ad hoc rogue alarms. Click the number in parentheses to access the Alarms page. Click an item under MAC address to view ad hoc details.

Most Recent Security Alarms

Displays the five most recent security alarms. Click the number in parentheses to access the Alarms page.

Rogue Access Points, Ad hoc Events, and Clients

This section describes security solutions for rogue devices. A rogue device is an unknown access point or client that is detected by managed access points in your network.

Controllers continuously monitor all nearby access points and automatically discover and collect information on rogue access points and clients. When a controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network.

Note The NCS consolidates all of the rogue access point data of the controller.

You can configure controllers to use RLDP on all access points or only on access points configured for monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded RF space, allowing monitoring without creating unnecessary interference and without affecting regular data access point functionality. If you configure a controller to use RLDP on all access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to either manually or automatically contain the detected rogue.

This section contains the following topics:

- Classifying Rogue Access Points, page 3-10
- Rogue Access Point Classification Types, page 3-11
- Adhoc Rogue, page 3-13

Classifying Rogue Access Points

Classification and reporting of rogue access points occurs through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states. You can create rules that enable the controller to organize and display rogue access points as Friendly, Malicious, or Unclassified.

Note The NCS consolidates all of the rogue access point data of the controller.

By default, none of the classification rules are enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, and unclassified) in the Alert state only.

Note Rule-based rogue classification does not apply to ad hoc rogues and rogue clients.

Note The 5500 series controllers support up to 2000 rogues (including acknowledged rogues); the 4400 series controllers, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch support up to 625 rogues; and the 2100 series controllers and Controller Network Module for Integrated Services Routers support up to 125 rogues. Each controller limits the number of rogue containments to three per radio (or six per radio for access points in monitor mode).

When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. The controller verifies that the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.

2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.
3. If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.
4. The controller applies the first rule based on priority. If the rogue access point matches the criteria specified by the rule, the controller classifies the rogue according to the classification type configured for the rule.
5. If the rogue access point does not match any of the configured rules, the controller classifies the rogue as Unclassified.
6. The controller repeats the previous steps for all rogue access points.
7. If RLDP determines that the rogue access point is on the network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can then manually contain the rogue (unless you have configured RLDP to automatically contain the rogue), which would change the rogue state to Contained. If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.
8. If desired, you can manually move the access point to a different classification type and rogue state.

As mentioned previously, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules, or you can manually move the unknown access point to a different classification type and rogue state. Table 3-6 shows the allowable classification types and rogue states from and to which an unknown access point can be configured.

Table 3-6 Allowable Classification Type and Rogue State Transitions

From	To
Friendly (Internal, External, Alert)	Malicious (Alert)
Friendly (Internal, External, Alert)	Unclassified (Alert)
Friendly (Alert)	Friendly (Internal, External)
Malicious (Alert, Threat)	Friendly (Internal, External)
Malicious (Contained, Contained Pending)	Malicious (Alert)
Unclassified (Alert, Threat)	Friendly (Internal, External)
Unclassified (Contained, Contained Pending)	Unclassified (Alert)
Unclassified (Alert)	Malicious (Alert)

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

Rogue Access Point Classification Types

Rogue access points classification types include the following:

- Malicious—Detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification. See the "Malicious Rogue Access Points" section on page 3-6 for more information.

- Friendly—Known, acknowledged, or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained. See the "Friendly Rogue APs" section on page 3-12 for more information. For more information on configuring friendly access point rules, see the "Configuring a Friendly Access Point Template" section on page 10-87.
- Unclassified—Rogue access point that are not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list. See the "Unclassified Rogue APs" section on page 3-13 for more information.

Malicious Rogue APs

Malicious rogue access points are detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification.

The Security dashboard of the NCS home page displays the number of malicious rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active malicious rogue access points.

Malicious rogue access point states include the following:

- Alert—Indicates that the access point is not on the neighbor list or part of the user-configured Friendly AP list.
- Contained—The unknown access point is contained.
- Threat—The unknown access point is found to be on the network and poses a threat to WLAN security.
- Contained Pending—Indicates that the containment action is delayed due to unavailable resources.
- Removed—This unknown access point was seen earlier but is not seen now.

Click an underlined number in any of the time period categories for detailed information regarding the malicious rogue access points. See the "Monitoring Rogue Access Points" section on page 5-91 for more information.

Friendly Rogue APs

Friendly rogue access points are known, acknowledged or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.

The Security dashboard of the NCS home page displays the number of friendly rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active friendly rogue access points.

Friendly rogue access point states include the following:

- Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. For example, the access points in your lab network.
- External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. For example, the access points belonging to a neighboring coffee shop.
- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.

Click an underlined number in any of the time period categories for detailed information regarding the friendly rogue access points. See the "Monitoring Rogue Access Points" section on page 5-91 for more information.

Unclassified Rogue APs

An unclassified rogue access point refers to a rogue access point that is not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list.

The Security dashboard of the NCS home page displays the number of unclassified rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active unclassified rogue access points.

Unclassified rogue access point states include the following:

- Pending—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point.
- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.
- Contained—The unknown access point is contained.
- Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

Click an underlined number in any of the time period categories for further information. See the "Monitoring Rogue Access Points" section on page 5-91.

Adhoc Rogue

If the MAC address of a mobile client operating in a ad hoc network is not in the authorized MAC address list, then it is identified as an ad hoc rogue.

Rogue Access Point Location, Tagging, and Containment

When the Cisco Unified Wireless Network Solution is monitored using the NCS, the NCS generates the flags as rogue access point traps and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the access points closest to each rogue access point. The next step is to mark them as **Known** or **Acknowledged** rogue access points (no further action), **Alert** rogue access points (watch for and notify when active), or **Contained** rogue access points (have between one and four access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

This built-in detection, tagging, monitoring, and containment capability enables system administrators to take the appropriate action:

- Locate rogue access points.
- Receive new rogue access point notifications, eliminating hallway scans.
- Monitor unknown rogue access points until they are eliminated or acknowledged.
- Determine the closest authorized access point, making directed scans faster and more effective.

- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment can be done for individual rogue access points by MAC address or can be mandated for all rogue access points connected to the enterprise subnet.
- Tag rogue access points:
  - Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or wireless LAN security.
  - Accept rogue access points when they do not compromise the LAN or wireless LAN security.
  - Tag rogue access points as unknown until they are eliminated or acknowledged.
  - Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

This section contains the following topics:

Detecting Access Points on a Network

Use the Detecting Access Points feature to view information about the Cisco lightweight access points that are detecting a rogue access point.

To access the Rogue AP Alarms details page, follow these steps:

Step 1 To display the Rogue AP Alarms page, do one of the following:

- Perform a search for rogue APs. See the "Using the Search Feature" section on page 2-33 for more information about the search feature.
- In the NCS home page, click the **Security** dashboard. This page displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the **Malicious AP** number link in the dashlet.

Step 2 In the Rogue AP Alarms page, click the Rogue MAC Address for the applicable rogue access point. The Rogue AP Alarms details page displays.

Step 3 From the Select a command drop-down list, choose **View Detecting AP on Network**.

Step 4 Click **Go**.

Click a list item to display data about that item:

- AP Name
- Radio
- Detecting AP Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- WEP—Enabled or disabled.
- WPA—Enabled or disabled.

- Pre-Amble—Long or short.
- RSSI—Received signal strength indicator in dBm.
- SNR—Signal-to-noise ratio.
- Containment Type—Type of containment applied from this access point.
- Containment Channels—Channels that this access point is currently containing.

Viewing Rogue Access Points by Controller

Use the Detecting Access Points feature to view information about the rogue access points by controller.

To access the Rogue AP Alarms details page, follow these steps:

Step 1 To display the Rogue AP Alarms page, do one of the following:

- Perform a search for rogue APs. See the "Using the Search Feature" section on page 2-33 for more information about the search feature.
- In the NCS home page, click the **Security** dashboard. This page displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the **Malicious AP** number link in the dashlet.

Step 2 In the Rogue AP Alarms page, click the Rogue MAC Address for the applicable rogue access point. The Rogue AP Alarms details page displays.

Step 3 From the Select a command drop-down list, choose **View AP Details by Controller**.

Step 4 Click **Go**.

Click a list item to display data about that item:

- Controller IP Address
- Detecting AP Name
- Radio
- Detecting AP Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- RSSI—Received Signal Strength Indicator in dBm.
- Classification—Indicates if the rogue AP classification.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point. See the "Rogue Access Point Classification Types" section on page 3-11 for additional information.
- On Network—Whether it belongs to this network "Yes" or "No".
- Containment Level—Indicates the containment level of the rogue access point or Unassigned (not contained).

- Last Updated Time

Working with Alarms

You can view, assign, and clear alarms and events on access points and mobility services engine using the NCS.

Details on how to have e-mail notifications of alarms sent to you is also described. This section contains the following topics:

Assigning and Unassigning Alarms

To assign and unassign an alarm to yourself, follow these steps:

Step 1 Perform an advanced search for access point alarms. See the "Using the Search Feature" section on page 2-33 for more information.

Step 2 Select the alarms that you want to assign to yourself by selecting their corresponding check boxes.

Note To unassign an alarm assigned to you, unselect the box next to the appropriate alarm. You cannot unassign alarms assigned to others.

Step 3 From the Select a command drop-down list, choose **Assign to Me** (or **Unassign**), and click **Go**.

If you choose **Assign to Me**, your username appears in the Owner column. If you choose **Unassign**, the username column becomes empty.

Deleting and Clearing Alarms

To delete or clear an alarm from a mobility services engine, follow these steps:

Step 1 In the Monitor > Alarms page, select the alarms that you want to delete or clear by selecting their corresponding check boxes.

Note If you delete an alarm, the NCS removes it from its database. If you clear an alarm, it remains in the NCS database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.

Step 2 From the Select a command drop-down list, choose **Delete** or **Clear**, and click **Go**.

Note To set up cleanup of old alarms and cleared alarms, choose **Administration > Settings > Alarms**.

Acknowledging Alarms

You might want certain alarms to be removed from the Alarms List. For example, if you are continuously receiving an interference alarm from a certain access point on the 802.11g interface, you might want to stop that access point from being counted as an active alarm on the page or any alarms list. In this scenario, you can find the alarm for the 802.11g interface in the Alarms list, select the check box, and choose **Acknowledge** from the Select a command drop-down list.

Now if the access point generates a new violation on the same interface, the NCS does not create a new alarm, and the page shows no new alarms. However, if the interference violation is created on another interface, such as 802.11a, a new alarm is created.

Any alarms, once acknowledged, do not show up on either the page or any alarm list page. Also, no e-mails are generated for these alarms after you have marked them as acknowledged. By default, acknowledged alarms are not included for any search criteria. To change this default, choose **Administration > Settings > Alarms** page and disable the Hide Acknowledged Alarms preference.

Note When you acknowledge an alarm, a warning displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Use the Administration > User Preferences page to disable this warning message.

You can also search for all previously acknowledged alarms to reveal the alarms that were acknowledged during the last seven days. The NCS automatically deletes cleared alerts that are more than seven days old so your results can only show activity for the last seven days. Until an existing alarm is deleted, a new alarm cannot be generated for any managed entity for which the NCS has already generated an alarm.

Monitoring Rogue Alarm Events

The Events page enables you to review information about rogue alarm events. The NCS generates an event when a rogue access point is detected or if you make manual changes to a rogue access point (such as changing its state). The Rogue AP Events list page displays all rogue access point events.

To access the Rogue AP Events list page, follow these steps:

Step 1 Do one of the following:

- Perform a search for rogue access point events using the Advanced Search feature of the NCS. See the "Using the Search Feature" section on page 2-33 for more information.
- In the Rogue AP Alarms details page, choose **Event History** from the Select a command drop-down list.

Step 2 The Rogue AP Events list page displays the following event information.

- Severity—Indicates the severity of the alarm.
- Rogue MAC Address—Click the rogue MAC address to view the Rogue AP Event Details page. See the "Viewing Rogue AP Event Details" section on page 3-18 for more information.

- Vendor—Rogue access point vendor name or Unknown.
- Classification Type—Malicious, Friendly, or Unclassified. See the "Rogue Access Point Classification Types" section on page 3-11 for more information.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Date/Time—The date and time that the event was generated.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point. See the "Rogue Access Point Classification Types" section on page 3-11 for additional information.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Viewing Rogue AP Event Details

To view rogue access point event details, follow these steps:

Step 1 In the Rogue AP Events list page, click the **Rogue MAC Address** link.

Step 2 The Rogue AP Events Details page displays the following information:

- Rogue MAC Address
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Classification Type—Malicious, Friendly, or Unclassified. See the "Rogue Access Point Classification Types" section on page 3-11 for more information.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point. See the "Rogue Access Point Classification Types" section on page 3-11 for additional information.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- Containment Level—Indicates the containment level of the rogue access point or Unassigned.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Created—The date and time that the event was generated.
- Generated By—The method by which the event was generated (such as Controller).
- Device IP Address

- Severity—Indicates the severity of the alarm.
- Message—Provides details of the current event.

Monitoring Adhoc Rogue Events

The Events page enables you to review information about ad hoc rogue events. The NCS generates an event when an ad hoc rogue is detected or if you make manual changes to an ad hoc rogue (such as changing its state). The Adhoc Rogue Events list page displays all ad hoc rogue events.

To access the Rogue AP Events list page, follow these steps:

Step 1 Do one of the following:

- Perform a search for ad hoc rogues events using the Advanced Search feature of the NCS. See the "Using the Search Feature" section on page 2-33 for more information.
- In the Adhoc Rogue Alarms details page, choose **Event History** from the Select a command drop-down list.

Step 2 The Rogue AP Events list page displays the following event information:

- Severity—Indicates the severity of the alarm.
- Rogue MAC Address—Click the rogue MAC address to view the Rogue AP Event Details page. See the "Viewing Adhoc Rogue Event Details" section on page 3-19 for more information.
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Date/Time—The date and time that the event was generated.
- State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Viewing Adhoc Rogue Event Details

To view rogue access point event details, follow these steps:

Step 1 In the Rogue AP Events list page, click the **Rogue MAC Address** link.

Step 2 The Rogue AP Events Details page displays the following information:

- Rogue MAC Address
- Vendor—Rogue access point vendor name or Unknown.

- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- Containment Level—Indicates the containment level of the rogue access point or Unassigned.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Created—The date and time that the event was generated.
- Generated By—The method by which the event was generated (such as Controller).
- Device IP Address
- Severity—Indicates the severity of the alarm.
- Message—Provides details of the current event.

Security Overview

The NCS provides a foundation that allows IT managers to design, control, secure, and monitor enterprise wireless networks from a centralized location.

The NCS provides the following tools for managing and enforcing wireless security configurations and policies within the Cisco wireless network infrastructure:

- Network security policy creation and enforcement, such as user authentication, encryption, and access control.
- Wireless infrastructure security configuration.
- Rogue detection, location, and containment.
- wireless Intrusion Prevention System (wIPS).
- Wireless IPS signature tuning and management.
- Management Frame Protection (MFP).
- Collaboration with Cisco wired Network IPS for monitoring and mitigating unauthorized or malicious wireless user activity.
- Comprehensive security event management and reporting.

Security Vulnerability Assessment

In Cisco Unified Wireless Network Version 5.1, an automated security vulnerability assessment is available to facilitate analysis for the overall wireless security posture of an enterprise, as well as to provide WLAN operators with real-time benchmarking of their security services configurations against industry best practices. The automated security vulnerability assessment provides the following:

- Proactive vulnerability monitoring of the entire wireless network.
- Comprehensive information on security vulnerabilities that could lead to loss of data, network intrusion, or malicious attack.
- Reduction in the time and expertise required to analyze and remedy weaknesses in wireless security posture.

The automated wireless vulnerability assessment audits the security posture of the entire wireless network for vulnerabilities. These vulnerabilities can result in:

- Unauthorized management access or using management protocols to compromise or adversely impact the network.
- Unauthorized network access, data leakage, man-in-the-middle, or replay attacks.
- Compromised or adverse impacts to the network through manipulation of network protocols and services, for example through denial of service (DoS) attacks.

The NCS automatically scans the entire network and compares settings against Cisco recommended and industry best practices for wireless security configurations. The automated wireless security assessment functions within the NCS scan wireless LAN controllers, access points, and network management interfaces for vulnerabilities in configuration settings, encryption, user authentication, infrastructure authentication network management, and access control.

Status of the wireless network security is graphically displayed to provide wireless network administrators with an easy-to-read dashboard of security events. The NCS displays the vulnerability assessment results through a Security Index on the NCS security dashboard. The Security Index summarizes the network security posture with a composite security score and prioritized summary of vulnerabilities. See the "Security Index" section on page 3-21" for more information.

Administrators can drill down to the Security Index Detailed Report if an event in the Security Summary warrants further investigation. The Security Index Detailed Report provides in-depth analysis of the vulnerabilities across the network. It also identifies optimal security settings and recommends changes that remedy the vulnerabilities. Any changes the administrator makes are reflected in an updated Security Index score. See the "Security Index Detailed Report" section on page 3-22" for more information.

Security Index

The Security Index gives an indication of the security of the NCS managed network. The security index is calculated by assigning weight to the various security configurations and displaying it in visual form. The combined weightages can vary from 0 to 100, where 0 signifies least secured and 100 maximum secured.

The weighting comes from the lowest scoring controller and the lowest scoring Location Server/Mobility Service Engine related security configurations that are maintained within the NCS itself. For example, the security index of the NCS managed network is equal to the lowest scoring controller plus the lowest scoring Location Server/Mobility Service Engine.

The following color scheme applies for the security index:

- Above or equal to 80—Green
- Below 80 but above or equal to 60—Yellow
- Below 60—Red

Note Guest WLANs are excluded from the WLANs. A WLAN which has web authentication or web passthrough enabled is identified as a guest WLAN.

The security index of the latest release is the benchmark for the required security configurations. For example, if AES encryption was not present in an earlier version of code, the index is reduced by the number associated with the AES encryption security configuration. Likewise, if new security configurations are introduced, the weighting would be altered.

The configurations stored in the NCS might not be up-to-date with the ones in the controllers unless the Refresh from Controller command is run from the NCS. You can run Security Index calculations from the Configuration Sync task to get the latest config data from all the controllers.

Top Security Issues

The Top Security Issues section displays the five top security issues. The View All and Devices links sort relevant columns and show a report of security issues occurring across all controllers. Click **View All** to open the Security Index Detailed Report. Click **Devices** to view the Security Index Controller Report.

- Security Index Detailed Report, page 3-22
- Security Index Controller Report, page 3-22
- Potential Security Issues, page 3-23

Security Index Detailed Report

The Security Index Detailed Report displays all security issues found across all controllers, location servers, and mobility service engines. It details problems found in a particular security configuration retrieved from the device. If a particular issue has been acknowledged (just like alarms), it is ignored when the next Configuration Sync task runs (if Security Index Calculation is enabled).

In some cases when an issue is acknowledged and it is ignored the next time the Configuration Sync task runs, the final security index score does not change. Some possible reasons for this might include the following:

- The acknowledged issue is on a controller which is not directly affecting the security index score (for instance, it is not the controller with the lowest score).
- The acknowledged issue is on a WLAN that is not directly affecting the security index score. Only the lowest scoring WLAN of the lowest scoring controller affects the security index score.

When SSH and Telnet are enabled on a controller and are both flagged as issues, the Telnet issue has a higher precedence than SSH. Even if SSH is acknowledged on the controller with the lowest score, no change would occur for the security index.

From the Select a command drop-down list, choose **Show All** to view all security issues (both acknowledged and unacknowledged). Choose **Show Unacknowledged** to only view unacknowledged security issues. This is the default view when View All is selected from the Security Summary page. Choose **Show Acknowledged** to only view acknowledged security issues.

Note For a user to acknowledge or unacknowledge security issues, the user must have “Ack and Unack Security Index Issues permission enabled".

Security Index Controller Report

This page shows the security violation report as a summary for each controller. By row, each controller shows the number of security issues that occurred on that controller and provides a link to all security issues.

If you click the number in the Security Issues Count column, the Security Index Detailed Report appears.

Potential Security Issues

Table 3-7 and Table 3-8 describe the potential security issues.

Table 3-7 Potential Security Issues

Controller Security Issue	Why is this an Issue?	What is the Solution?
WLAN SSID on the controller has a weak authentication method.	Weak authentication method for a WLAN which can be broken by using tools available online if WLAN packets are sniffed.	Use the most secured authentication method and one that is WPA+WPA2.
WLAN SSID on the controller has a weak authentication method (CKIP) configured.	Weak authentication method for a WLAN.	Use the most secured authentication method and one that is WPA+WPA2.
WLAN SSID on the controller has no user authentication configured.	No authentication method is a clear security risk for a WLAN.	Configure strong authentication methods such as WPA+WPA2.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits with Key Permutation) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits with MMH) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits with MMH and Key Permutation) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (WEP 104 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits with MMH) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.

Table 3-7 Potential Security Issues (continued)

Controller Security Issue	Why is this an Issue?	What is the Solution?
WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits with Key Permutation) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits with MMH and Key Permutation) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (WEP 40 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (WEP 128 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (TKIP) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has no encryption configured.	No encryption method is a clear security risk for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (WEP 104 bits) configured.	Weak encryption method for WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has no key management methods configured (applicable only for WPA+WPA2).	A key management method enhances the security of keys; without one, WLAN is less secure.	Configure at least one key management methods such as CCKM.
WLAN SSID on the controller has MFP Client Protection set to “Optional”.	With MFP Client Protection set to optional for a WLAN, authenticated clients might not be shielded from spoofed frames.	Set MFP Client Protection to “Required” to protect against clients connecting to a rogue access point.
WLAN SSID on the controller has MFP Client Protection set to “Disabled”.	With MFP Client Protection set to disabled for a WLAN, authenticated clients might not be shielded from spoofed frames.	Set MFP Client Protection to “Required” to protect against clients connecting to a rogue access point.
WLAN SSID interface is set to “management” on the controller.	As recommended from SAFE, user traffic should be separated from management traffic.	WLAN interface should not be set to “management” on the controller.
Interface set to one which is VLAN for a WLAN.	As recommended from SAFE, user traffic should be separated from VLAN traffic.	WLAN needs its interface to be set to one which is neither management nor one which has a VLAN.

Table 3-7 Potential Security Issues (continued)

Controller Security Issue	Why is this an Issue?	What is the Solution?
WLAN SSID on the controller has "Client Exclusion" disabled.	With Client Exclusion policies disabled, an attacker is able to continuously try to access the WLAN network.	Enable "Client Exclusion" to secure against malicious WLAN client behavior.
WLAN SSID on the controller has "Broadcast SSID" enabled.		Disable "Broadcast SSID" to secure your wireless network.
WLAN SSID on the controller has "MAC Filtering" disabled.		Enable "MAC Filtering" to secure your wireless network.
Protection Type is set to "AP Authentication" on the controller.	When AP Authentication is set, an access point checks beacon/probe response frames in neighboring access points to see if they contain an authenticated information element (IE) that matches that of the RF group. This provides some security but does not cover all management frames and is open to alteration by rogue access points.	Set Protection Type to "Management Frame Protection (MFP)" on the controller.
Protection Type is set to "None" of the controller.	No security for 802.11 management messages passed between access points and clients.	Set Protection Type to "Management Frame Protection (MFP)" on the controller.
Radio type is configured to detect rogues only on DCA channels.	Rogue detection, if done only on a subset of country/all channels, is less secure than one that is done on country/all channels.	Configure radio types 802.11a/n and 802.11b/g/n to detect rogues on country channels or all channels.
Radio type is configured to detect rogues on neither country channels nor DCA channels.	Rogue detection, if not configured on country nor DCA channels, is less secure than when done on country/all channels.	Configure radio types 802.11a/n and 802.11b/g/n to detect rogues on country channels or all channels.
The rogue policy to detect and report ad hoc networks is disabled on the controller.	With detection and reporting of ad hoc networks turned off, ad hoc rogues go undetected.	Enable the rogue policy to detect and report ad hoc networks.
"Check for all Standard and Custom Signatures" is disabled on the controller.	If check for all Standard and Custom Signatures is disabled, various types of attacks in incoming 802.11 packets would go undetected. various types of attacks in incoming 802.11 packets would go undetected.	Check for all Standard and Custom Signatures needs to be turned on to identify various types of attacks in incoming 802.11 packets.
Some of the Standard Signatures are disabled on the controller.	If only some of the Standard Signatures are disabled,	Enable all Standard Signatures on the controller.

Table 3-7 Potential Security Issues (continued)

Controller Security Issue	Why is this an Issue?	What is the Solution?
The "Excessive 802.11 Association Failures" Client Exclusion Policy is disabled on the controller.	Excessive failed association attempts can consume system resources and launch potential a denial of service attack to the infrastructure.	Enable the "Excessive 802.11 Association Failures" Client Exclusion Policy on the controller.
The "Excessive 802.11 Authentication Failures" Client Exclusion Policy is disabled on the controller.	Excessive failed authentication attempts can consume system resources and launch potential Denial of Service attack to the infrastructure.	Enable the "Excessive 802.11 Authentication Failures" Client Exclusion Policy on the controller.
The "Excessive 802.1X Authentication Failures" Client Exclusion Policy is disabled on the controller.	Excessive 802.1X failed authentication attempts can consume system resources and launch potential denial of service attack to the infrastructure.	Excessive 802.1X Authentication Failures Client Exclusion Policy must be enabled to prevent denial of service attack to the infrastructure.
The "Excessive 802.11 Web Authentication Failures" Client Exclusion Policy is disabled on the controller.	If Excessive 802.11 Web failed web authentication attempts can consume system resources and launch potential denial of service attack to the infrastructure.	Enable the "Excessive 802.11 Web Authentication Failures" Client Exclusion Policy on the controller.
The "IP Theft or IP Reuse" Client Exclusion Policy is disabled on the controller.	If IP Theft or Reuse Client Exclusion Policy is disabled, then an attacker masquerading as another client would not be disallowed.	Enable the "IP Theft or IP Reuse" Client Exclusion Policy on the controller.
No CIDS Sensor configured on the controller.	If no enabled IDS Sensor is configured, then IP-level attacks would not be detected.	Configure at least one CIDS Sensor on the controller.
Controller is configured with default community strings for SNMP v1/v2.	If SNMP V1 or V2 with default Community is configured then it is open to easy attacks because default communities are well known.	Use SNMPv3 with Auth and Privacy Types.
Controller is configured with non-default community strings for SNMP v1/v2.	SNMP V1 or V2 with non-default Community is slightly more secure than default Community but still less secure than SNMP V3.	Use SNMPv3 with Auth and Privacy types.
SNMPv3 is configured with a default user on the controller.	Using a default user makes SNMP V3 connections less secure.	Use a non-default username for SNMPv3 with Auth and Privacy Types.
SNMPv3 is configured with either no Auth or Privacy Type on the controller.	SNMP V3 with either Auth or Privacy Type set to none reduces the security of SNMP V3 connection.	Use SNMPv3 with Auth and Privacy Types to secure your wireless network.

Table 3-7 Potential Security Issues (continued)

Controller Security Issue	Why is this an Issue?	What is the Solution?
HTTP (Web Mode enabled but Secure Web Mode disabled) is enabled on the controller.	HTTP is less secure than HTTPS.	Enable HTTPS (both Web Mode and Secure Web Mode) on the controller.
Telnet is enabled on the controller.	If telnet is enabled, then the controller is at risk of being hacked into.	Disable telnet on the controller.
SSH is disabled and timeout value is set to zero on the controller.	If SSH is enabled and timeout is zero then the controller has risk of being hacked into.	Enable SSH with non-zero timeout value on the controller.
Telnet is enabled on the AP.	If telnet is enabled, then the access point is at risk of being hacked into.	Disable Telnet on all access points.
SSH is enabled on the AP.		Disable SSH on all the access points.
At least one of the APs is configured with default username or password.	If default password is configured, then access points are more susceptible to connections from outside the network.	Configure a non-default username and strong password for all access points associated to the controller.

Table 3-8 Potential Security Issues

Location Server/ Mobility Server Engine Security Issue	Why is this an Issue?	What is the Solution?
HTTP is enabled on the location server.	HTTP is less secure than HTTPS.	Enable HTTPS on the location server.
A location server user has a default password configured.	If default password is configured, then Location Server/ Mobility Server Engine is more susceptible to connections from outside the network.	Configure a strong password for the location server users.
HTTP is enabled on the mobility services engine.	HTTP is less secure than HTTPS.	Enable HTTPS on the mobility services engine.
A mobility services engine user has default password configured.	If default password is configured, then Location Server/ Mobility Server Engine is more susceptible to connections from outside the network.	Configure a strong password for the users on the mobility services engine.
wIPS Service is not enabled on the mobility services engine.	Your network is vulnerable to advanced security threats.	Deploy wIPS Service to protect your network from advanced security threats.

Switch Port Tracing

Currently, the NCS provides rogue access point detection by retrieving information from the controller. The rogue access point table is populated with any detected BSSID addresses from any frames that are not present in the neighbor list. At the end of a specified interval, the contents of the rogue table are sent to the controller in a CAPWAP Rogue AP Report message. With this method, the NCS would simply gather the information received from the controllers; but with software Release 5.1, you can incorporate switch port tracing of Wired Rogue Access Point Switch Ports. This enhancement allows you to react to found wired rogue access points and prevent future attacks. The trace information is available only in the NCS log and only for rogue access points, not rogue clients.

Note Rogue Client connected to the Rogue Access point information is used to track the switch port to which the Rogue Access point is connected in the network.

Note If you try to set tracing for a friendly or deleted rogue, a warning message appears.

Note For Switch Port Tracing to successfully trace the switch ports using SNMP v3, all of the OIDs should be included in the SNMP v3 view and VLAN content should be created for each VLAN in the SNMP v3 group.

Establishing Switch Port Tracing

To establish switch port tracing, follow these steps:

Step 1 In the NCS home page, click the **Security** dashboard.

Step 2 In the Rogue APs and Adhoc Rogues group box, click the number URL which specifies the number of rogues in the last hour, last 24 hours, or total active.

Step 3 Choose for which rogue you are setting switch port tracking by clicking the URL in the MAC Address column. The Alarms > Rogue AP details page opens.

Step 4 From the Select a command drop-down list, choose **Trace Switch Port**. The Trace Switch Port page opens, and the NCS runs a switch port trace.

When one or more searchable MAC addresses are available, the NCS uses CDP to discover any switches connected up to two hops away from the detecting access point. The MIBs of each CDP discovered switch is examined to see if it contains any of the target MAC addresses. If any of the MAC addresses are found, the corresponding port number is returned and reported as the switch port of a rogue.

Integrated Security Solutions

The Cisco Unified Wireless Network Solution also provides these integrated security solutions:

- Cisco Unified Wireless Network Solution operating system security is built around a robust 802.1X authorization, authentication, and accounting (AAA) engine, which enables operators to rapidly configure and enforce a variety of security policies across the Cisco Unified Wireless Network Solution.
- The controllers and access points are equipped with system-wide authentication and authorization protocols across all ports and interfaces, maximizing system security.
- Operating system security policies are assigned to individual wireless LANs, and access points simultaneously broadcast all (up to 16) configured wireless LANs. These policies can eliminate the need for additional access points, which can increase interference and degrade system throughput.
- Operating system security uses the RRM function to continually monitor the air space for interference and security breaches and notify the operator when they are detected.
- Operating system security works with industry-standard AAA servers, making system integration simple and easy.
- The Cisco Intrusion Detection System/Intrusion Protection System (IDS/IPS) instructs controllers to block certain clients from accessing the wireless network when attacks involving these clients are detected.
- The operating system security solution offers comprehensive Layer 2 and Layer 3 encryption algorithms, which typically require a large amount of processing power. Rather than assigning the encryption tasks to yet another server, the controller can be equipped with a VPN/enhanced security module that provides extra hardware required for the most demanding security configurations.

Using the NCS to Convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 Mode

To convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 LWAPP transport mode using the NCS user interface, follow these steps:

Note Cisco-based lightweight access points do not support Layer 2 LWAPP mode. These access points can only be run with Layer 3.

Note This procedure causes your access points to go offline until the controller reboots and the associated access points reassociate to the controller.

Step 1 Make sure that all controllers and access points are on the same subnet.

Note You must configure the controllers and associated access points to operate in Layer 2 mode before completing the conversion.

Step 2 Log into the NCS user interface. Then follow these steps to change the LWAPP transport mode from Layer 3 to Layer 2:

a. Choose **Configure > Controllers** to navigate to the All Controllers page.

b. Click the desired IP address of a controller to display the *IP Address* > Controller Properties page.

c. From the left sidebar menu, click **System > General** to display the *IP Address* > General page.

d. Change LWAPP transport mode to **Layer2,** and click **Save**.

e. If the NCS displays the following message, click **OK**:

```
Please reboot the system for the LWAPP Mode change to take effect.
```

Step 3 To restart your Cisco Unified Wireless Network Solution, follow these steps:

a. Return to the *IP Address* > Controller Properties page.

b. Click **System > Commands** to display the *IP Address* > Controller Commands page.

c. Under Administrative Commands, choose **Save Config To Flash**, and click **Go** to save the changed configuration to the controller.

d. Click **OK** to continue.

e. Under Administrative Commands, choose **Reboot**, and click **Go** to reboot the controller.

f. Click **OK** to confirm the save and reboot.

Step 4 After the controller reboots, follow these steps to verify that the LWAPP transport mode is now Layer 2:

a. Click **Monitor > Controllers** to navigate to the Controllers > Search Results page.

b. Click the desired IP address of a controller to display the Controllers > *IP Address* > Summary page.

c. Under General, verify that the current LWAPP transport mode is Layer2.

You have completed the LWAPP transport mode conversion from Layer 3 to Layer 2. The operating system software now controls all communications between controllers and access points on the same subnet.

Configuring a Firewall for the NCS

When an NCS server and an NCS user interface are on different sides of a firewall, they cannot communicate unless the following ports on the firewall are open to two-way traffic:

- 80 (for initial http)
- 69 (tftp)
- 162 (trap port)
- 443 (https)

Open these ports to configure your firewall to allow communications between an NCS server and an NCS user interface.

Access Point Authorization

To view a list of authorized access points along with the type of certificate that an access point uses for authorization, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click one of the URLs in the IP address column.

Step 3 From the left sidebar menu, choose **Security > AP/MSE Authorization**.

Step 4 The AP Policies portion of the page indicates whether the authorization of access points is enabled or disabled. It also indicates whether the acceptance of self-signed certificates (SSC APs) is enabled or disabled. Normally, access points can be authorized either by AAA or certificates. (SSC is only available for 4400 and 200 controllers.)

To change these values, choose **Edit AP Policies** from the Select a command drop-down list, and click **Go**.

Step 5 The AP Authorization List portion shows the radio MAC address of the access point, certificate type, and key hash. To add a different authorization entry, choose **Add AP/MSE Auth Entry** from the Select a command drop-down list, and click **Go**.

Step 6 From the drop-down list, choose a template to apply to this controller, and click **Apply**. To create a new template for access point authorization, click the **click here** link to get redirected to the template creation page. See the "Configuring an Access Point or MSE Authorization Template" section on page 10-63 for steps on creating a new template.

Management Frame Protection (MFP)

Management Frame Protection (MFP) provides security for the otherwise unprotected and unencrypted 802.11 management messages passed between access points and clients. MFP provides both infrastructure and client support.

- Infrastructure MFP—Protects management frames by detecting adversaries who are invoking denial of service attacks, flooding the network with associations and probes, interjecting as rogue access points, and affecting network performance by attacking the QoS and radio measurement frames. It also provides a quick and effective means to detect and report phishing incidents.

  Specifically, infrastructure MFP protects 802.11 session management functions by adding message integrity check information elements (MIC IEs) to the management frame emitted by access points (and not those emitted by clients), which are then validated by other access points in the network. Infrastructure MFP is passive. It can detect and report intrusions but has no means to stop them.

- Client MFP—Shields authenticated clients from spoofed frames, preventing many of the common attacks against wireless LANs from becoming effective. Most attacks, such as deauthentication attacks, revert to simply degrading performance by contending with valid clients.

  Specifically, client MFP encrypts management frames sent between access points and Cisco Compatible Extension clients so that both access points and clients can take preventive action by dropping spoofed class 3 management frames (that is, management frames passed between an access point and a client that is authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect the following types of class 3 unicast management frames: disassociation, deauthentication, and QoS (WMM) action. Client MFP is active. It can protect a client-access point session from the most common type of denial of service attack. It protects class 3 management frames by using the same encryption method used for the data frames of the session. If a frame received by the access point or client fails decryption, it is dropped, and the event is reported to the controller.

  To use client MFP, clients must support Cisco Compatible Extensions (Version 5) MFP and must negotiate WPA2 using either TKIP or AES-CCMP. EAP or PSK might be used to obtain the PMK. CCKM and controller mobility management are used to distribute session keys between access points or Layer 2 and Layer 3 fast roaming.

To prevent attacks against broadcast frames, access points supporting Cisco Compatible Extensions (version 5) do not emit any broadcast class 3 management frames (such as disassociation, deauthentication, or action). Compatible extensions clients (Version 5) and access points must discard broadcast class 3 management frames.

Client MFP supplements infrastructure MFP rather than replacing it because infrastructure MFP continues to detect and report invalid unicast frames sent to clients that are not client-MFP capable, as well as invalid class 1 and 2 management frames. Infrastructure MFP is applied only to management frames that are not protected by client MFP.

Infrastructure MFP consists of three main components:

- Management frame protection—The access point protects the management frames it transmits by adding a MIC IE to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving access point configured to detect MFP frames to report the discrepancy.
- Management frame validation—In infrastructure MFP, the access point validates every management frame it receives from other access points in the network. It ensures that the MC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an access point that is configured to transmit MFP frames, it reports the discrepancy to the network management system. For the timestamps to operate properly, all controllers must be Network Transfer Protocol (NTP) synchronized.
- Event reporting—The access point notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and reports the results through SNMP traps to the network management system.

Note Client MFP uses the same event reporting mechanisms as infrastructure MFP.

Infrastructure MFP is enabled by default and can be disabled globally. When you upgrade from a previous software release, infrastructure MFP is disabled globally if access point authentication is enabled because the two features are mutually exclusive. After infrastructure MFP is enabled globally, signature generation (adding MICs to outbound frames) can be disabled for selected WLANs, and validation can be disabled for selected access points.

You set MFP in the WLAN template. See the "Configuring WLAN Templates" section on page 10-22.

Guidelines for Using MFP

Follow these guidelines for using MFP:

- MFP is supported for use with Cisco Aironet lightweight access points, except for the 1500 series mesh access points.
- Lightweight access points support infrastructure MFP in local and monitor modes and in REAP and FlexConnect modes when the access point is connected to a controller. They support client MFP in local, FlexConnect, and bridge modes.
- Client MFP is supported for use only with Cisco Compatible Extensions (Version 5) clients using WPA2 with TKIP or AES-CCMP.
- Non-Cisco Compatible Extensions (Version 5) clients might associate to a WLAN if client MFP is disabled or optional.

Configuring Intrusion Detection Systems (IDS)

The Cisco Intrusion Detection System/Intrusion Prevention System (IDS/IPS) instructs controllers to block certain clients from accessing the wireless network when attacks involving these clients are detected. This system offers significant network protection by helping to detect, classify, and stop threats including worms, spyware/adware, network viruses, and application abuse. Two methods are available to detect IDS attacks:

- IDS sensors (for Layer 3)
- IDS signatures (for Layer 2)

Viewing IDS Sensors

When the sensors identify an attack, they alert the controller to shun the offending client. When you add a new IDS sensor, you register the controller with that IDS sensor so that the sensor can send shunned client reports to the controller. The controller also polls the sensor periodically.

To view IDS sensors, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose a controller by clicking an IP address.

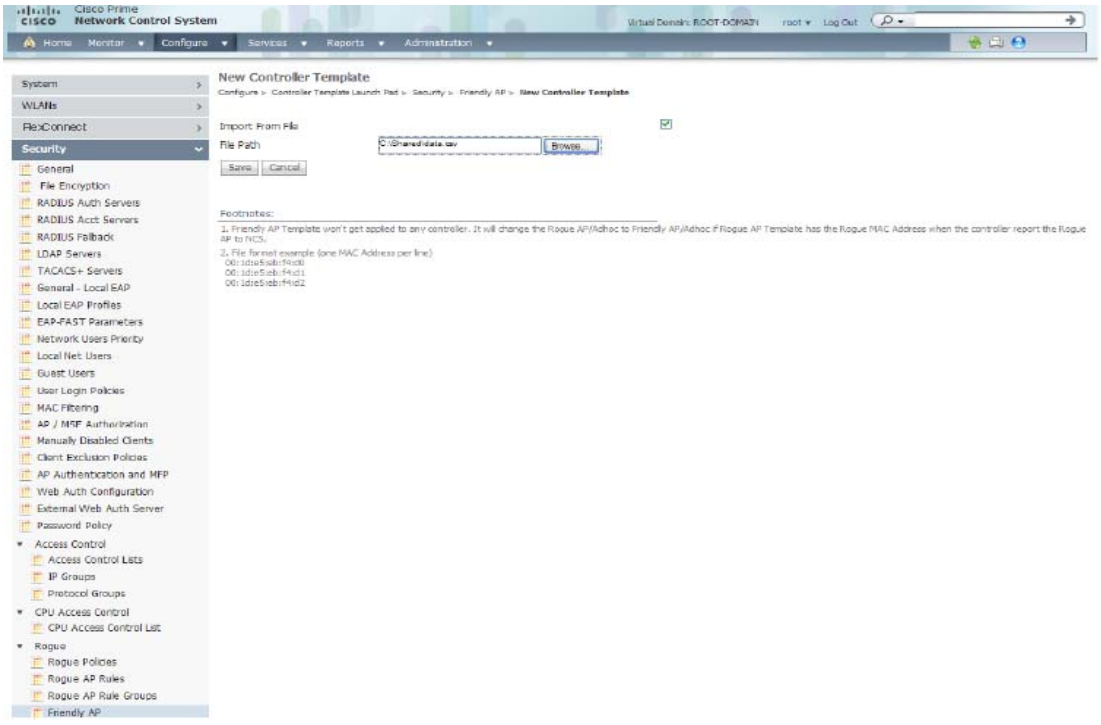
Step 3 From the left sidebar menu, choose **Security > IDS Sensor Lists**. The IDS Sensor page appears. This page lists all of the IDS sensors that have been configured for this controller.

Configuring IDS Signatures

You can configure *IDS signatures*, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller. If an attack is detected, an appropriate mitigation action is initiated.

Cisco supports 17 standard signatures on the controller as shown on the Standard Signatures and Custom Signatures page (see Figure 3-3). To open this page, choose **Configure > Controllers**, select a controller IP address, and then choose **Security > Wireless Protection Policies > Standard Signatures** from the left sidebar menu.

Figure 3-3 Standard Signatures Page



These signatures are divided into six main groups. The first four groups contain management signatures, and the last two groups contain data signatures:

- Broadcast deauthentication frame signatures—During a broadcast deauthentication frame attack, a hacker sends an 802.11 deauthentication frame to the broadcast MAC destination address of another client. This attack causes the destination client to disassociate from the access point and lose its connection. If this action is repeated, the client experiences a denial of service. When the broadcast deauthentication frame signature (precedence 1) is used to detect such an attack, the access point listens for clients transmitting broadcast deauthentication frames that match the characteristics of the signature. If the access point detects such an attack, it alerts the controller. Depending on how your system is configured, the offending device is contained so that its signals no longer interfere with authorized clients, or the controller forwards an immediate alert to the system administrator for further action, or both.
- NULL probe response signatures—During a NULL probe response attack, a hacker sends a NULL probe response to a wireless client adapter. As a result, the client adapter locks up. When a NULL probe response signature is used to detect such an attack, the access point identifies the wireless client and alerts the controller. The NULL probe response signatures include the following:
  - NULL probe resp 1 (precedence 2)
  - NULL probe resp 2 (precedence 3)
- Management frame flood signatures—During a management frame flood attack, a hacker floods an access point with 802.11 management frames. The result is a denial of service to all clients associated or attempting to associate to the access point. This attack can be implemented with different types of management frames: association requests, authentication requests, reassociation requests, probe requests, disassociation requests, deauthentication requests, and reserved management subtypes.

When a management frame flood signature is used to detect such an attack, the access point identifies management frames matching the entire characteristics of the signature. If the frequency of these frames is greater than the value of the frequency set in the signature, an access point that hears these frames triggers an alarm. The controller generates a trap and forwards it to the NCS.

The management frame flood signatures include the following:

- Assoc flood (precedence 4)
- Auth flood (precedence 5)
- Reassoc flood (precedence 6)
- Broadcast probe flood (precedence 7)
- Disassoc flood (precedence 8)
- Deauth flood (precedence 9)
- Reserved mgmt 7 (precedence 10)
- Reserved mgmt F (precedence 11)

The reserved management frame signatures 7 and F are reserved for future use.

- EAPOL flood signature—During an EAPOL flood attack, a hacker floods the air with EAPOL frames containing 802.1X authentication requests. As a result, the 802.1X authentication server cannot respond to all of the requests and fails to send successful authentication responses to valid clients. The result is a denial of service to all affected clients. When the EAPOL flood signature (precedence 12) is used to detect such an attack, the access point waits until the maximum number of allowed EAPOL packets is exceeded. It then alerts the controller and proceeds with the appropriate mitigation.
- NetStumbler signatures—NetStumbler is a wireless LAN scanning utility that reports access point broadcast information (such as operating channel, RSSI information, adapter manufacturer name, SSID, WEP status, and the latitude and longitude of the device running NetStumbler when a GPS is attached). If NetStumbler succeeds in authenticating and associating to an access point, it sends a data frame with the following strings, depending on the NetStumbler version listed in Table 3-9.

Table 3-9 NetStumbler Versions

Version	String
3.2.0	“Flurble gronk bloopit, bnip Frundletrune”
3.2.3	“All your 802.11b are belong to us”
3.3.0	Sends white spaces

When a NetStumbler signature is used to detect such an attack, the access point identifies the offending device and alerts the controller. The NetStumbler signatures include the following:

- NetStumbler 3.2.0 (precedence 13)
- NetStumbler 3.2.3 (precedence 14)
- NetStumbler 3.3.0 (precedence 15)
- NetStumbler generic (precedence 16)

- Wellenreiter signature—Wellenreiter is a wireless LAN scanning and discovery utility that can reveal access point and client information. When the Wellenreiter signature (precedence 17) is used to detect such an attack, the access point identifies the offending device and alerts the controller.

This section provides the instructions to configure signatures and contains the following topics:

Uploading IDS Signatures

To upload IDS signatures from the controller, follow these steps:

Step 1 Obtain a signature file from Cisco (hereafter called a *standard signature file*). You can also create your own signature file (hereafter called a *custom signature file*) by following the "Downloading IDS Signatures" section on page 3-37.

Step 2 You can configure a TFTP server for the signature download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable. However, if you want to put the TFTP server on a different network while the management port is down, add a static route if the subnet where the service port resides has a gateway (config route add *IP address of TFTP server*).
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the NCS because built-in TFTP server of the NCS and third-party TFTP server use the same communication port.

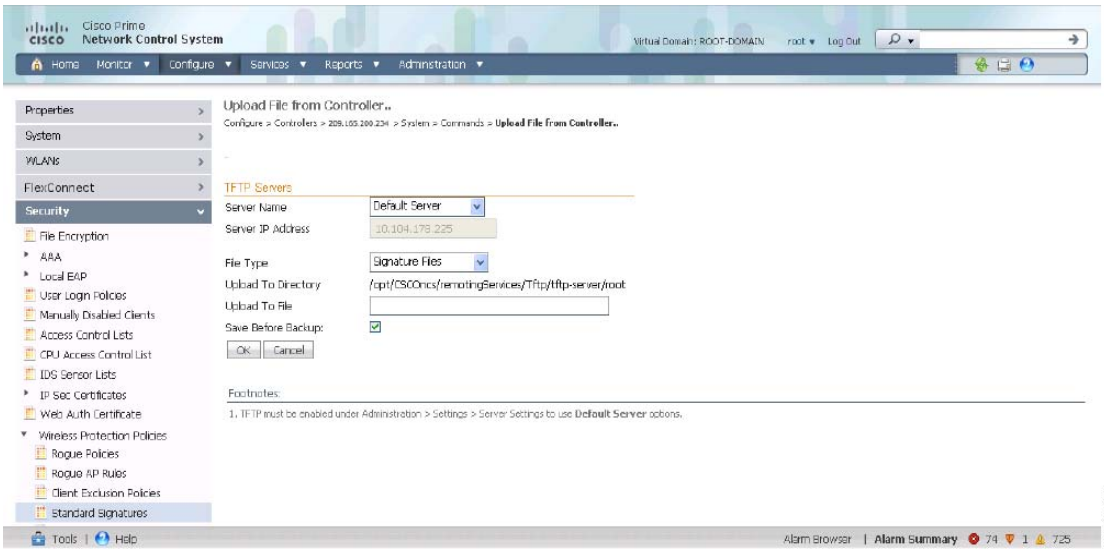
Step 3 Choose **Configure > Controllers**.

Step 4 Choose a controller by clicking an IP address.

Step 5 From the left sidebar menu, choose **Security** and then choose **Standard Signatures** or **Custom Signatures**.

Step 6 From the Select a command drop-down list, choose **Upload Signature Files from Controller**. Figure 3-4 shows the page that appears.

Figure 3-4 Uploading Signature File



Step 7 Specify the TFTP server name being used for the transfer.

Step 8 If the TFTP server is new, enter the TFTP IP address at the Server IP Address field.

Step 9 Choose **Signature Files** from the File Type drop-down list.

Step 10 The signature files are uploaded to the root directory which was configured for use by the TFTP server. You can change to a different directory at the Upload to File field (this field only shows if the Server Name is the default server). The controller uses this local file name as a base name and then adds *_std.sig* as a suffix for standard signature files and *_custom.sig* as a suffix for custom signature files.

Step 11 Click **OK**.

Downloading IDS Signatures

If the standard signature file is already on the controller but you want to download customized signatures to it, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose a controller by clicking an IP address.

Step 3 Choose **System > Commands**.

Step 4 From the Upload/Download Commands drop-down list, choose **Download IDS Signatures**, and click **Go**.

Step 5 Copy the signature file (*.sig) to the default directory on your TFTP server.

Step 6 Choose **local machine** from the File is Located On field. If you know the filename and path relative to the root directory of the server, you can also choose TFTP server.

Step 7 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries field.

Step 8 Enter the maximum amount of time, in seconds, before the controller times out while attempting to download the signature file in the Timeout field.

Step 9 The signature files are uploaded to the c:\tftp directory. Specify the local file name in that directory or use the Browse button to navigate to it. A "revision" line in the signature file specifies whether the file is a Cisco-provided standard signature file or a site-tailored custom signature file (custom signature files must always have revision=custom).

Step 10 If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the Server File Name is populated for you and retried. The local machine option initiates a two-step operation. First, the local file is copied from the workstation of the administrator to the built-in TFTP server of the NCS. Then the controller retrieves that file. For later operations, the file is already in the TFTP directory of the NCS server, and the download web page now automatically populates the filename.

Step 11 Click **OK**.

Enabling or Disabling IDS Signatures

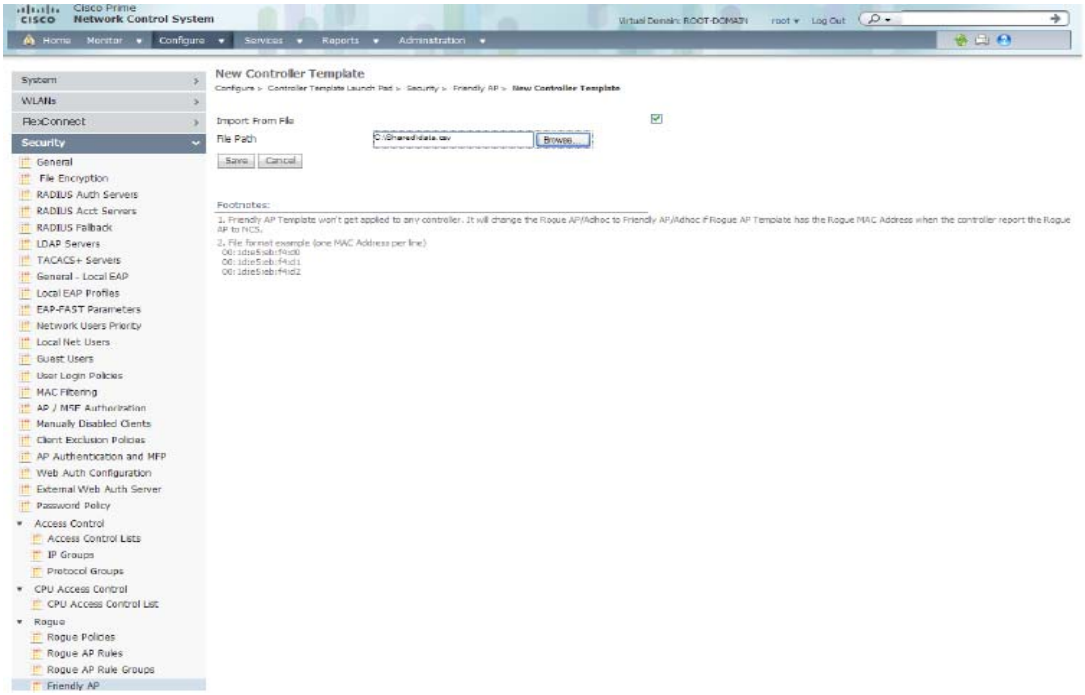
To enable or disable IDS signature, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose a controller by clicking an IP address.

Step 3 From the left sidebar menu, choose **Security** and then choose **Standard Signatures** or **Custom Signatures**. Figure 3-5 shows a sample of the page that appears.

Figure 3-5 Checking for Standard Signatures



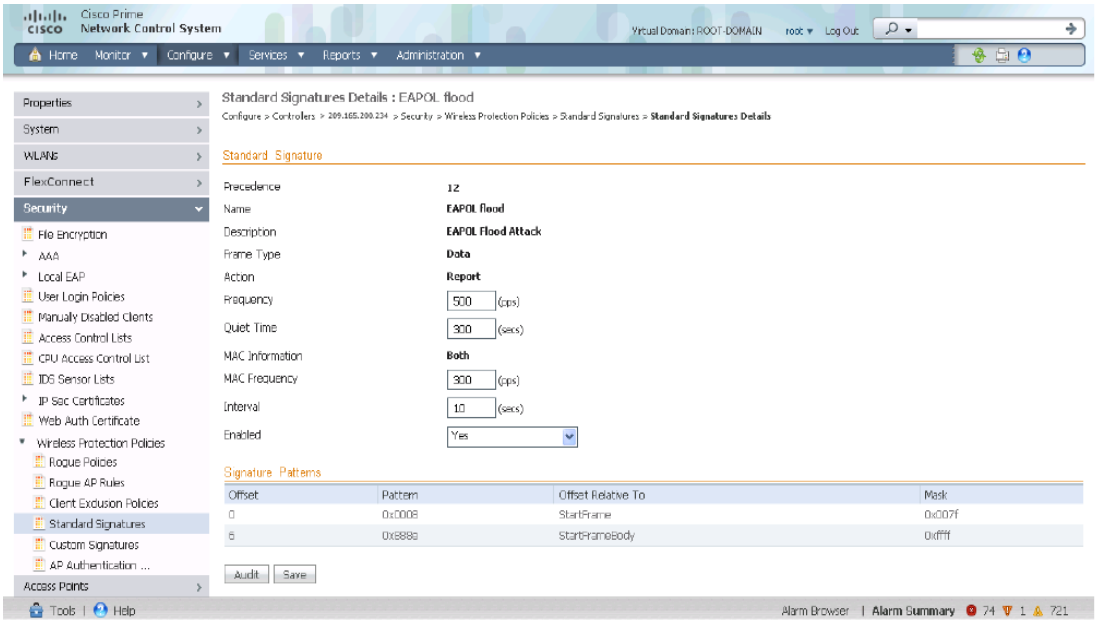
Step 4 To enable or disable an individual signature, click in the **Name** column for the type of attack you want to enable or disable. Figure 3-6 shows a sample of a detailed signature screen.

The Standard Signature Parameters page shows the list of Cisco-supplied signatures that are currently on the controller. The Custom Signatures page shows the list of customer-supplied signatures that are currently on the controller. The following information is displayed either in the signature page or the detailed signature page:

- Precedence—The order, or precedence, in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Description—A more detailed description of the type of attack that the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. One possibility is *None*, where no action is taken, and another is *Report*, to report the detection.
- Frequency—The signature frequency, or the number of matching packets per interval that must be identified at the detecting access point level before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value is 50 packets per interval.
- Quiet Time—The length of time (in seconds) after which no attacks have been detected at the individual access point level, and the alarm can stop. This time appears only if the MAC information is all or both. The range is 60 to 32,000 seconds, and the default value is 300 seconds.
- MAC Information—Whether the signature is to be tracked per network or per MAC address or both at the detecting access point level.
- MAC Frequency—The signature MAC frequency, or the number of matching packets per interval that must be identified at the controller level before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value is 30 packets per interval.

- Interval—Enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds, and the default value is 1 second.
- Enable—Select this to enable this signature to detect security attacks or unselect it to disable this signature.
- Signature Patterns—The pattern that is being used to detect a security attack.

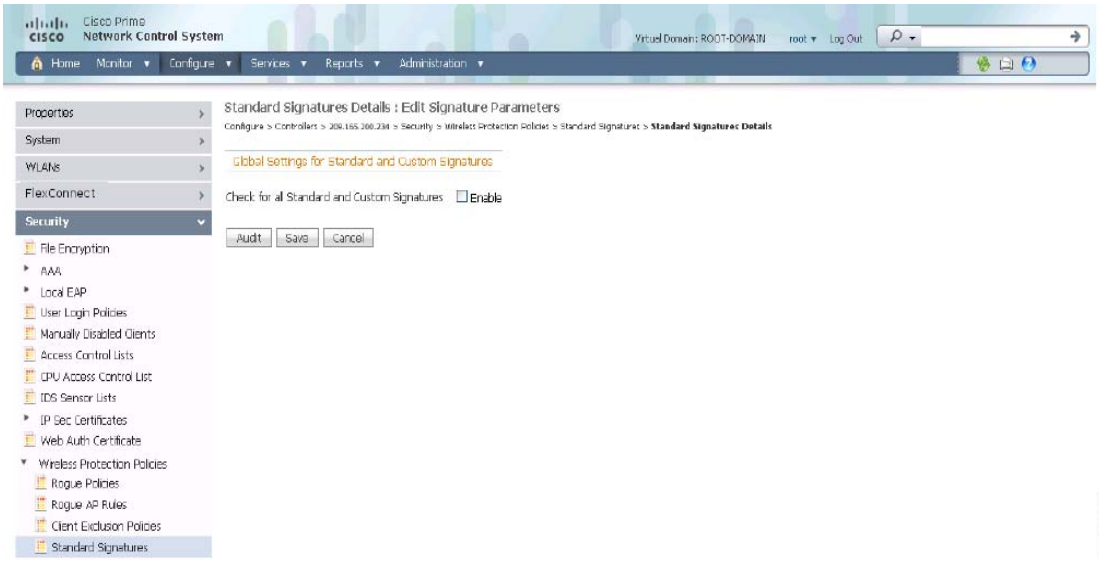
Figure 3-6 Standard Signature



Step 5 From the Enabled yes or no drop-down list, choose **yes**. Because you are downloading a customized signature, you should enable the files named with the _custom.sgi and disable the standard signature with the same name but differing suffix. (For example, if you are customizing broadcast probe flood, you want to disable broadcast probe flood in the standard signatures but enable it in custom signatures.)

Step 6 To enable all standard and custom signatures currently on the controller, choose **Edit Signature Parameters** (from the screen in Figure 3-5) from the Select a command drop-down list, and choose **Go**. The Edit Signature Parameters page appears (see Figure 3-7).

Figure 3-7 Global Setting for Standard and Custom Signature



Step 7 Select the Check for All Standard and Custom Signatures field, **Enable** check box. This enables all signatures that were individually selected as enabled in Step 5. If this check box remains unselected, all files are disabled, even those that were previously enabled in Step 5. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.

Step 8 Click **Save**.

Enabling Web Login

With web authentication, guests are automatically redirected to web authentication pages when they launch their browsers. Guests gain access to the WLAN through this web portal. Wireless LAN administrators using this authentication mechanism should have the option of providing unencrypted or encrypted guest access. Guest users can then log into the wireless network using a valid username and password, which is encrypted with SSL. Web authentication accounts might be created locally or managed by a RADIUS server. The Cisco Wireless LAN controllers can be configured to support a web authentication client. See the "Configuring a Web Authentication Template" section on page 10-68 to create a template that replaces the Web authentication page provided on the controller.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the controller on which to enable web authentication by clicking an IP address URL in the IP Address column.

Step 3 From the left sidebar menu, choose **Security > AAA > Web Auth Configuration**.

Step 4 Choose the appropriate web authentication type from the drop-down list. The choices are default internal, customized web authentication, or external.

- If you choose default internal, you can still alter the page title, message, and redirect URL, as well as choose whether the logo appears. Continue to Step 5.
- If you choose customized web authentication, skip to the "Downloading Customized Web Authentication" section on page 3-42.
- If you choose external, you need to enter the URL you want to redirect to after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page.

Step 5 Select the **Logo Display** check box if you want your company logo to display.

Step 6 Enter the title you want displayed on the Web authentication page.

Step 7 Enter the message you want displayed on the Web authentication page.

Step 8 In the Customer Redirect URL field, provide the URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page.

Step 9 Click **Save**.

Downloading Customized Web Authentication

You can download a customized Web authentication page to the controller. A customized web page is created to establish a username and password for user web access.

When downloading customized web authentication, these strict guidelines must be followed:

- A username must be provided.
- A password must be provided.
- A redirect URL must be retained as a hidden input item after extracting from the original URL.
- The action URL must be extracted and set from the original URL.
- Scripts to decode the return status code must be included.
- All paths used in the main page should be of relative type.

Before downloading, if you chose the customized web authentication option in Step 4 of the previous section, follow these steps:

Step 1 Click the preview image to download the sample login.html bundle file from the server. See Figure 3-8 for an example of the login.html file. The downloaded bundle is a .TAR file.

Figure 3-8 Login.html

Step 2 Open and edit the login.html file and save it as a .tar or .zip file.

Note You can edit the text of the Submit button with any text or HTML editor to read "Accept terms and conditions and Submit."

Step 3 Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the NCS because the built-in TFTP server of the NCS and third-party TFTP server use the same communication port.

Step 4 Click **here** in the "After editing the HTML you might click **here** to redirect to the Download Web Auth Page" link to download the .tar or .zip file to the controller(s). The Download Customized Web Auth Bundle to Controller page appears.

Note The IP address of the controller to receive the bundle and the current status are displayed.

Step 5 Choose **local machine** from the File is Located On field. If you know the filename and path relative to the root directory of the server, you can also choose TFTP server.

Note For a local machine download, either .zip or .tar file options exists, but the NCS does the conversion of .zip to .tar automatically. If you chose a TFTP server download, only .tar files are specified.

Step 6 Enter the maximum amount of time in seconds before the controller times out while attempting to download the file in the Timeout field.

Step 7 The NCS Server Files In field specifies where the NCS server files are located. Specify the local file name in that directory or use the Browse button to navigate to it. A "revision" line in the signature file specifies whether the file is a Cisco-provided standard signature file or a site-tailored custom signature file (custom signature files must always have revision=custom).

Step 8 If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the Server File Name is populated. The local machine option initiates a two-step operation. First, the local file is copied from the workstation of the administrator to the built-in TFTP server of the NCS. Then the controller retrieves that file. For later operations, the file is already in the TFTP directory of the NCS server, and the download web page now automatically populates the filename.

Step 9 Click **OK**.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the Server File Name is populated for you.

Step 10 After completing the download, you are directed to the new page and able to authenticate.

Connecting to the Guest WLAN

To connect to the guest central WLAN to complete the web authentication process, follow these steps: See the "Creating Guest User Accounts" section on page 6-10 for more explanation of a guest user account.

Step 1 When you are set for open authentication and are connected, browse to the virtual interface IP address (such as /209.165.200.225/login.html).

Step 2 When the NCS user interface displays the Login page, enter your username and password.

Note All entries are case sensitive.

The lobby ambassador has access to the templates only to add guest users.

Certificate Signing Request (CSR) Generation

To generate a Certificate Signing Request (CSR) for a third-party certificate using the NCS, see the Appendix D, "Certificate Signing Request (CSR) Generation for a Third-Party Certificate on a Cisco Prime Network Control System (NCS)."

CHAPTER 3

Performing Maintenance Operations

You can perform the actions at the system level, such as updating system softwares or downloading certificates that can be used with many items.

This chapter describes the system level tasks to perform with Cisco NCS. It contains the following sections:

Information About Maintenance Operations

A system-level task is a collection of tasks that relate to operations that apply to the NCS database as a whole. System tasks also include restoring the NCS database. For more information, see the "Restoring the NCS Database" section on page 3-8.

Performing System Tasks

This sections describes how to use the NCS to perform system-level tasks. This section contains the following topics:

Adding a Controller to the NCS Database

To add a controller to the NCS database, follow these steps:

Note We recommend that you manage controllers through the controller dedicated service port for improved security. However, when you manage controllers that do not have a service port (such as 2000 series controllers) or for which the service port is disabled, you must manage those controllers through the controller management interface.

Step 1 Log into the NCS user interface.

Step 2 Choose **Configure > Controllers** to display the All Controllers page.

Step 3 From the Select a command drop-down list, choose **Add Controller**, and click **Go**.

Step 4 In the Add Controller page, enter the controller IP address, network mask, and required SNMP settings.

Step 5 Click **OK**. The NCS displays a Please Wait dialog box while it contacts the controller and adds the current controller configuration to the NCS database. It then returns you to the Add Controller page.

Step 6 If the NCS does not find a controller at the IP address that you entered for the controller, the Discovery Status dialog displays this message:

```
No response from device, check SNMP.
```

Check these settings to correct the problem:

- The controller service port IP address might be set incorrectly. Check the service port setting on the controller.
- The NCS might not have been able to contact the controller. Make sure that you can ping the controller from the NCS server.
- The SNMP settings on the controller might not match the SNMP settings that you entered in the NCS. Make sure that the SNMP settings configured on the controller match the settings that you entered in the NCS.

Step 7 Add additional controllers if desired.

Using the NCS to Update System Software

To update controller (and access point) software using the NCS, follow these steps:

Step 1 Enter the **ping** *ip-address* command to be sure that the NCS server can contact the controller. If you use an external TFTP server, enter the **ping** *ip-address* command to be sure that the NCS server can contact the TFTP server.

Note When you are downloading through a controller distribution system (DS) network port, the TFTP server can be on the same or a different subnet because the DS port is routable.

Step 2 Choose **Configure > Controllers** to navigate to the All Controllers page.

Step 3 Select the check box of the desired controller, choose **Download Software (TFTP or FTP)** from the Select a command drop-down list, and click **Go**. The NCS displays the Download Software to Controller page.

Step 4 If you use the built-in NCS TFTP server, choose **Default Server** from the Server Name drop-down list box. If you use an external TFTP server, choose **New** from the Server Name drop-down list box and add the external TFTP server IP address.

Step 5 Enter the file path and server file name in their respective text boxes (for example, AS_2000_*release*.aes for 2000 series controllers). The files are uploaded to the root directory which was configured for use by the TFTP server. You can change to a different directory.

Note Be sure that you have the correct software file for your controller.

Step 6 Click **Download**. The NCS downloads the software to the controller, and the controller writes the code to flash RAM. As the NCS performs this function, it displays its progress in the Status field.

Downloading Vendor Device Certificates

Each wireless device (controller, access point, and client) has its own device certificates. For example, the controller is shipped with a Cisco-installed device certificate. This certificate is used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific device certificate, it must be downloaded to the controller.

To download a vendor-specific device certificate to the controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 You can download the certificates in one of two ways:

a. Select the check box of the controller you choose.

b. Choose **Download Vendor Device Certificate** from the Select a command drop-down list, and click **Go**.

or

a. Click the URL of the desired controller in the IP Address column.

b. Choose **System > Commands** from the left sidebar menu.

c. Choose **TFTP** or **FTP** in the Upload/Download Command section.

d. Choose **Download Vendor Device Certificate** from the Upload/Download Commands drop-down list, and click **Go**.

Step 3 In the Certificate Password text box, enter the password which was used to protect the certificate.

Step 4 Specify if the certificate to download is on the TFTP server or on the local machine. If it is on the TFTP server, the name must be supplied in the Server File Name field. If the certificate is on the local machine, you must specify the file path in the Local File Name field using the **Choose File** button.

Step 5 Enter the TFTP server name in the Server Name field. The default is for the NCS server to act as the TFTP server.

Step 6 Enter the server IP address.

Step 7 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 8 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 9 In the Local File Name text box, enter the directory path of the certificate.

Step 10 Click **OK**.

Downloading Vendor CA Certificates

Controllers and access points have a certificate authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate might be used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific CA certificate, it must be downloaded to the controller. To download vendor CA certificate to the controller, follow the instructions:

Step 1 Choose **Configure > Controllers**.

Step 2 You can download the certificates in one of two ways:

a. Select the check box of the controller you choose.

b. Choose **Download Vendor CA Certificate** from the Select a command drop-down list, and click **Go**.

or

a. Click the URL of the desired controller in the IP Address column.

b. Choose **System > Commands** from the left sidebar menu.

c. Choose **Download Vendor CA Certificate** from the Upload/Download Commands drop-down list, and click **Go**.

Step 3 Specify if the certificate to download is on the TFTP server or on the local machine. If it is on the TFTP server, the name must be supplied in the Server File Name field in Step 9. If the certificate is on the local machine, you must specify the file path in the Local File Name field in Step 8 using the Browse button.

Step 4 Enter the TFTP server name in the Server Name field. The default is for the NCS server to act as the TFTP server.

Step 5 Enter the server IP address.

Step 6 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 7 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 8 In the Local File Name text box, enter the directory path of the certificate.

Step 9 Click **OK**.

Using the NCS to Enable Long Preambles for SpectraLink NetLink Phones

A radio preamble (sometimes called a *header*) is a section of data at the head of a packet. It contains information that wireless devices need when sending and receiving packets. Short preambles improve throughput performance, so they are enabled by default. However, some wireless devices, such as SpectraLink NetLink phones, require long preambles.

To optimize the operation of SpectraLink NetLink phones on your wireless LAN, to use the NCS to enable long preambles, follow these steps:

Step 1 Log into the NCS user interface.

Step 2 Choose **Configure > Controllers** to navigate to the All Controllers page.

Step 3 Click the IP address of the desired controller.

Step 4 From the left sidebar menu, choose **802.11b/g/n > Parameters**.

Step 5 If the *IP Address* > 802.11b/g/n Parameters page shows that short preambles are enabled, continue to the next step. However, if short preambles are disabled, which means that long preambles are enabled, the controller is already optimized for SpectraLink NetLink phones, and you do not need to continue this procedure.

Step 6 Enable long preambles by unselecting the **Short Preamble** check box.

Step 7 Click **Save** to update the controller configuration.

Step 8 To save the controller configuration, choose **System > Commands** from the left sidebar menu, choose **Save Config To Flash** from the Administrative Commands drop-down list, and click **Go**.

Step 9 To reboot the controller, choose **Reboot** from the Administrative Commands drop-down list and click **Go**.

Step 10 Click **OK** when the following message appears.

```
Please save configuration by clicking "Save Config to flash". Do you want to continue
rebooting anyways?
```

The controller reboots. This process might take some time, during which the NCS loses its connection to the controller.

Note You can view the controller reboot process with a command-line interface session.

Creating an RF Calibration Model

If you would like to further refine the NCS Location tracking of client and rogue access points across one or more floors of a building, you have the option of creating an RF calibration model that uses physically collected RF measurements to fine-tune the location algorithm. When you have multiple floors in a building with the same physical layout as the calibrated floor, you can save time calibrating the remaining floors by using the same RF calibration model for the remaining floors.

The calibration models are used as RF overlays with measured RF signal characteristics that can be applied to different floor areas. This allows the Cisco Unified Wireless Network Solution installation team to lay out one floor in a multi-floor area, use the RF calibration tool to measure and save the RF characteristics of that floor as a new calibration model, and apply that calibration model to all the other floors with the same physical layout.

Performing the NCS Operations

This section contains the following topics:

Verifying the Status of the NCS

This section provides instructions for checking the status of the NCS. To check the status of the NCS. You can check the status at any time, follow these steps:

Step 1 Log into the system as admin.

Step 2 Using the CARS command-line interface, enter the **NCS status** command.

The command-line interface displays messages indicating the status of the NCS.

Stopping the NCS

This section provides instructions for stopping the NCS. You can stop the NCS at any time. To stop the NCS, follow these steps:

Note If any users are logged in when you stop the NCS, their NCS sessions stop functioning.

Step 1 Log into the system as admin.

Note To see which version of NCS you currently have installed, enter **show application version NCS**.

Step 2 Using the CARS command-line interface, enter the **NCS stop** command.

The command-line interface displays messages indicating that NCS is stopping.

Backing Up the NCS Database

This section provides instructions for backing up the NCS database. You can schedule regular backups through the NCS user interface or manually initiate a backup.

Note Machine specific settings (such as FTP enable and disable, FTP port, FTP root directory, TFTP enable and disable, TFTP port, TFTP root directory, HTTP forward enable and disable, HTTP port, HTTPS port, report repository directory, and all high availability settings) are not included in the backup and restore function if the backup is restored to a different device.

This section contains the following topics:

Scheduling Automatic Backups

To schedule automatic backups of the NCS database, follow these steps:

Step 1 Log into the NCS user interface.

Step 2 Choose **Administration > Background Tasks** to display the Scheduled Tasks page.

Step 3 Click the **NCS Server Backup** task to display the NCS Server Backup page.

Step 4 Select the **Enabled** check box.

Step 5 At the Backup Repository field, Choose an existing backup repository, or click **Create** to create a new repository.

Step 6 If you are backing up in remote location, select the **FTP Repository** check box. You need to enter the FTP location, username, and password of the remote machine.

Step 7 In the Interval (Days) text box, enter a number representing the number of days between each backup. For example, 1 = a daily backup, 2 = a backup every other day, 7 = a weekly backup, and so on.

Range: 1 to 360

Default: 7

Step 8 In the Time of Day text box, enter the time when you want the backup to start. It must be in this format: *hh*:*mm* AM/PM (for example: 03:00 AM).

Note Backing up a large database affects the performance of the NCS server. Therefore, we recommend that you schedule backups to run when the NCS server is idle (for example, in the middle of the night).

Step 9 Click **Submit** to save your settings. The backup file is saved as a .zip file in the *ftp-install-dir*/ftp-server/admin/NCSBackup directory using this format: *dd-mmm-yy_ hh-mm-ss*.zip (for example, 11-Nov-05_10-30-00.zip).

Performing a Manual Backup

To back up the NCS database, follow these steps:

Note You do not need to shut down Oracle or the platform to perform a backup.

Step 1 Log into the system as admin.

Step 2 Create a local or remote backup directory for the NCS database with no spaces in the name (for example, mkdir NCS1.0.X.X_Backup).

Note Make sure that the directory name does not contain spaces. Spaces can generate errors.

Note If it is a remote backup location, you MUST specify the correct FTP location (For example, ftp://hostname/location) and user credentials.

Step 3 You can perform a backup using the command-line interface.

Step 4 Run either of these commands to perform a manual backup:

- Back up the appliance and application to the repository (local or remote) by entering the following command:

  backup *testbackup* repository *backup_repo*

- Back up the application only to the repository (local or remote) by entering the following command:

  backup *testbackup* repository *backup_repo* application *NCS*

The command-line interface displays messages indicating the status of the backup.

Restoring the NCS Database

This section provides instructions for restoring the NCS database. This section contains the following topics:

Restoring the NCS Database

If you are restoring the NCS database in a high availability environment, see the "Restoring the NCS Database in a High Availability Environment" section on page 3-9. To restore the NCS database from a backup file. follow these steps:

Step 1 To view all local repository backups, enter the following command:

```
show repository backup_repo
```

Note If possible, stop all the NCS user interfaces to stabilize the database.

Step 2 Manually shut down the platform.

Step 3 Using the command-line interface, perform one of the following:

- Restore the appliance and application backup by entering the following command:

  ```
  restore testbackup-yymmdd-xxxx.tar.gpg repository backup_repo
  ```

- Restore only the application backup by entering the following command:

  ```
  restore testbackup-yymmdd-xxxx.tar.gpg repository backup_repo application NCS
  ```

Step 4 Click **Yes** if a message appears indicating that the NCS is running and needs to be shut down.

Note If the restore process shuts down the NCS, a restart is attempted after a successful restore. The appliance then restarts and you have to again login and restart the dbserver and the platform manually as admin (make sure you do not start with dbclean, else you lose your recently restored data).

The command-line interface displays messages indicating that the NCS database is being restored.

Restoring the NCS Database in a High Availability Environment

During installation, you were prompted to determine if a secondary NCS server would be used for high availability support to the primary NCS server. If you opted for this high availability environment and enabled it in the Administration > High Availability page, the status appears as HA enabled. Before restoring a database, you must convert the status to HA not configured.

Note If you attempt to restore the database while the status is set to HA enabled, unexpected results might occur.

To change the status from HA enabled to HA not configured, follow one of these procedures:

- Click the **Remove** button in the HA Configuration page (Administration > High Availability).
- Restart the primary server. Go to the secondary HealthMonitor graphical user interface (https://<SecondaryNCS>:8082), and click **Failback**.
  - Use this method when one of the following instances has occurred:

The primary server is down and failover has not been executed, so then the secondary server is in SecondaryLostPrimary state.

or

The primary server is down and failover has already executed, so then the secondary server is in the SecondaryActive state.

The primary server is now in HA Not Configured mode, and you can safely restore the database.

Uninstalling NCS

This section provides instructions for uninstalling the NCS. You can uninstall the NCS at any time, even while the NCS is running.

To uninstall the NCS, follow these steps:

Step 1 Stop the NCS.

Step 2 Log into the system as admin.

Step 3 Using the CARS command-line interface, enter the **application remove NCS** command.

Step 4 Click **Yes** to continue the uninstall process.

Upgrading WCS to NCS

This section provides instructions for upgrading to the NCS. If you are upgrading to the NCS in a high availability environment, see the "Upgrading the NCS in a High Availability Environment" section on page 3-11.

Note The NCS supports data migration in the WCS Releases 7.0.164.3, 7.0.172.0, and 7.0.220.0. If you do not have either release of the WCS, you must upgrade to either the WCS 7.0.164.3 or 7.0.172.0 or 7.0.220.0 first and then follow the migration steps.

To Upgrade from the WCS to the NCS, perform the following:

Step 1 Stop the WCS server.

Step 2 Enter the export command to export all the WCS data in to a export file. For Linux, enter the **export.sh all** command and for windows enter the **export.bat all** command.

Note While upgrading from the WCS to the NCS, on running the export command, you might encounter a "could not reserve enough space" error. If you encounter this error then access either the export.bat (for Windows OS) or export.sh (for Linux OS) file and replace the instance of -Xmx1024m with -Xmx512m.

Step 3 Copy the export .zip file (for example, wcs.zip) in to a local repository folder.

Step 4 Log in to the NCS as admin and stop the NCS server using the **NCS stop** command.

Step 5 Configure the repository in the NCS appliance using the repository command:

```
ncs-appliance/admin# configure
ncs-appliance/admin(config)# repository wcs-ftp-repo
ncs-appliance/admin(config-Repository)# url ftp://209.165.200.227//
ncs-appliance/admin(config-Repository)# user ftp-user password plain ftp-user
```

Note Make sure wcs.zip is listed for the **show repository repositoryname** command. For tftp, if directory listing is not enabled, then restore fails. This is an expected behavior and the **show repository** command produces an error message.

```
ncs-appliance/admin# show repository wcs-ftp-repo
wcs.zip
ncs-appliance/admin# show repository wcs-tftp-repo
% Protocol does not support listing directories
```

Step 6 Enter the **NCS migrate** command to restore the WCS database.

```
ncs-appliance/admin# NCS migrate wcs-data wcs.zip repository wcs-ftp-repo
```

Using the noclientstats option, no client count and client statistics data are migrated to the NCS. By default no WCS events are migrated.

Step 7 Run the **NCS start** command to start the NCS server after the upgrade is completed.

Step 8 Login to the NCS User Interface using the admin and the admin password.

Note The client count, client summary, client throughput, client traffic, rogue AP, adhoc rogues, new adhoc rogues, PCI details, PCI summary and security summary reports, dashboard customizations, client station information and its statistics, all WCS events, RADIUS/TACACS server IP and credentials, and the admin password are not migrated from the WCS to the NCS. Make sure you enable the RADIUS/TACACS server as AAA mode in **Administration > AAA > AAA Mode Settings** page and click **Save**.

Upgrading the NCS in a High Availability Environment

If you have a primary and secondary NCS, follow these steps for a successful upgrade:

Step 1 You must first remove the HA configuration with the following steps:

a. Log in to the primary NCS server.

b. Choose **Administration > High Availability**, and choose HA Configuration from the left sidebar menu.

c. Click **Remove** to remove the HA configuration.

Note It might take a few minutes for the remove to complete.

Step 2 You must first upgrade the secondary NCS with the following steps:

a. Shut down the secondary NCS. See the "Stopping the NCS" section on page 3-6 for more information.

Note You can use **NCS stop** for a graceful shut down. A graceful shut down does not trigger the automatic failover.

b. Perform an upgrade on the secondary NCS.

c. Start the secondary NCS.

Note It attempts to reconnect to the primary NCS, but a version mismatch error is returned.

Step 3 Upgrade the primary NCS.

a. Shut down the primary NCS. See the "Stopping the NCS" section on page 3-6 for more information.

b. Perform an upgrade on the primary NCS.

c. Start the primary NCS.

Step 4 Enable HA again on the primary NCS.

a. Login to the primary NCS server.

b. Choose Administration > High Availability and select HA Configuration from the left sidebar menu.

c. Enter the HA configuration settings and click **Save** to enable high availability.

Upgrading the Network

Network upgrades must follow a recommended procedure so that databases can remain synchronized with each other. For example, You cannot upgrade the controller portion of the network to a newer release but maintain the current NCS version and not upgrade it. The supported order of upgrade is NCS first, followed by the controller, and then any additional devices.

Reinitializing the Database

If you need to reset the database because of a synchronization problem or a corruption of some type, enter **NCS db reinitdb** to reinitialize the database.

Recovering the NCS Password

You can change the NCS application root user or FTP user password. To recover the passwords and regain access to the NCS, follow these steps:

Note If you are a Linux user, you must be the admin user to run the command.

Step 1 Log in to the NCS command-line interface as an admin user.

Step 2 Enter the following command:

NCS password root password *password*

Where *password* is the root user login password. You can enter a password not exceeding 80 characters.

Example of the command usage:

```
NCS-appliance/admin# NCS password root password ?

<WORD>  Type in root user login password (Max Size - 80)
```

You should now be able to login to the NCS web interface with the new root password.

CHAPTER 5

Monitoring Devices

Information About Monitoring

This chapter describes how to use the Cisco NCS to monitor Cisco WLAN Solution device configurations. This chapter contains the following sections:

Monitoring Controllers

Choose **Monitor > Controllers** to access the controller list page. Click a controller IP address to view its details.

This section contains the following topics:

Searching Controllers

Use the NCS Search feature to find specific controllers or to create and save custom searches.

For a controller search, you can search using the following fields:

Table 5-1 Search Controllers

Fields	Description
Search for controller by	Choose **All Controllers**, **IP Address**, **Controller Name**, or **Network**. **Note** Search fields might change depending on the selected category. When applicable, enter the additional field or filter information to help identify the Search By category.
Enter Controller IP Address	This field only appears if you select IP Address from the Search for controller by field.
Enter Controller Name	This field only appears if you select Controller Name from the Search for controller by field.
Audit Status	Choose one of the following from the drop-down list: – **All Status** – **Mismatch**—Configuration differences were found between NCS and controller during the last audit. – **Identical**—No configuration differences were found during the last audit. – **Not Available**—Audit status is unavailable.

See the following topics for additional information:

- Using the Search Feature, page 2-33
- Quick Search, page 2-33
- Advanced Search, page 2-34
- Saved Searches, page 2-46

Viewing a List of Controllers

Choose **Monitor > Controllers** or perform a controller search to access the controller list page.

Note See the "Advanced Search" section on page 2-34 for more information on performing an advanced search.

The data area of this page contains a table with the following columns.

Table 5-2 Controller List Details

Fields	Description
IP Address	Local network IP address of the controller management interface. Click an IP address in the list to display the controller details.
Controller Name	Name of the controller.
Location	The geographical location (such as a campus or building).
Mobility Group Name	Name of the controller mobility or WPS group.
Reachability Status	Reachable or Unreachable. Click the title to toggle from ascending to descending order.

Click the title to toggle from ascending to descending order. To add, remove, or reorder columns in the table, click the **Edit View** link to go to the Edit View page.

Configuring the Controller List Display

The **Edit View** page allows you to add, remove, or reorder columns in the Controllers table.

To edit the available columns in the Controllers table, follow these steps:

Step 1 Choose **Monitor > Controllers**.

Step 2 Click the **Edit View** link.

Step 3 To add an additional column to the controllers table, click to highlight the column heading in the left list. Click **Show** to move the heading to the right list. All items in the right list are displayed in the Controllers table.

Step 4 To remove a column from the Controllers table, click to highlight the list heading in the right list. Click **Hide** to move the heading to the left list. All items in the left list are not displayed in the Controllers table.

Step 5 Use the buttons to specify the order in which the information appears in the table. Highlight the desired list heading and click **Up** or **Down** to move it higher or lower in the current list.

Step 6 Click **Reset** to restore the default view.

Step 7 Click **Submit** to confirm the changes.

Monitoring System Parameters

This section provides the detailed information regarding monitoring controller system parameters and contains the following topics:

- Monitoring System Summary, page 5-4

Monitoring System Summary

This page displays a summary of the controller parameters with a graphic displaying the status of the controller. The graphic of the front of the controller shows front-panel ports (click a port to go to Monitor Controllers > *IPaddr* > Ports > General for information about that port). You can find the links to alarms, events and access points details related to the controller.

You can access this page in the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address.
- Choose **Monitor > Access Points**, click a list item under AP Name, then click **Registered Controller**.
- Choose **Configure > Access Points**, choose a list item under AP Name, then click **Registered Controller**.

Click **Controllers** in the page title to view a list of all the controllers. See the "Viewing a List of Controllers" section on page 5-2.

Table 5-3 lists the Monitoring System Summary page fields.

Table 5-3 Monitoring System Summary Page Fields

Field	Description
General	
IP Address	Local network IP address of the controller management interface.
Name	User-defined name of the controller.
Device Type	Type of controller.
UP Time	Time in days, hours and minutes since the last reboot.
System Time	Time used by the controller.
Internal Temperature	The temperature of the controller.
Location	User-defined physical location of the controller.
Contact	Contact person or the owner of the controller.
Total Client Count	Total number of clients currently associated with the controller.
Current CAPWAP Transport Mode	Control and Provisioning of Wireless Access Points (CAPWAP) protocol transport mode. Communications between controllers and access points. Choose **Layer 2** or **Layer 3**.
Power Supply One	If the power supply is available and operation. This is only for 4400 series controller.
Power Supply Two	If the power supply is available and operation. This is only for 4400 series controller.
Inventory	

Table 5-3 Monitoring System Summary Page Fields (continued)

Field	Description
Software Version	The operating system release.version.dot.maintenance number of the code currently running on the controller.
Emergency Image Version	An image version of the controller.
Description	Description of the inventory item.
Model No	Specifies the machine model as defined by the Vital Product Data.
Serial No	Unique serial number for this controller.
Burned-in MAC Address	The burned-in MAC address for this controller.
Number of APs Supported	The maximum number of access points supported by the controller.
Gig Ethernet/Fiber Card	Displays the presence or absence of the optional 1000BASE-T/1000BASE-SX GigE card.
Crypto Card One	Displays the presence or absence of an enhanced security module which enables IPsec security and provides enhanced processing power. **Note** By default, the enhanced security module is not installed on a controller. Maximum number of crypto cards that can be installed on a Cisco Wireless LAN controller: – Cisco 2000 Series—None – Cisco 4100 Series—One – Cisco 4400 Series—Two
Crypto Card Two	Displays the presence or absence of a second enhanced security module.
GIGE Port(s) Status	Up or Down. Click to review the status of the port.
Unique Device Identifier (UDI)	
Name	Product type. Chassis for controller and Cisco AP for access points.
Description	Description of controller and might include number of access points.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial No	Unique product serial number.
Utilization	
CPU Utilization	Displays a graph of the maximum, average, and minimum CPU utilization over the specified amount of time.
Memory Utilization	Displays a graph of the maximum, average, and minimum memory utilization over the specified amount of time.

Monitoring Spanning Tree Protocol

The Spanning Tree Protocol (STP) is a link management protocol. Cisco WLAN Solution implements the IEEE 802.1D standard for media access control bridges.

Spanning tree algorithm provides redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail.

You can access this page in the following ways:

- Choose **Monitor > Controllers**, select an IP address, and choose **System > Spanning Tree Protocol** from the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **System > Spanning Tree Protocol** from the left sidebar menu.

Note The controllers that do not support Spanning Tree Protocol are WISM, 2500, 5500, 7500 and SMWLC.

Table 5-4 lists the Spanning Tree Protocol page fields.

Table 5-4 Spanning Tree Protocol Fields Page Fields

Field	Description
General	
Spanning Tree Specification	An indication of what version of the Spanning Tree Protocol is being run. IEEE 802.1D implementations return 'IEEE 802.1D'. If future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value is defined.
Spanning Tree Algorithm	Specifies if this controller participates in the Spanning Tree Protocol. Might be enabled or disabled by choosing the corresponding line in the drop-down list. The factory default is disabled.
Priority	The value of the writable portion of the Bridge ID, that is, the first two octets of the (8 octet long) Bridge ID. The other (last) 6 octets of the Bridge ID are given by the value of Bridge MAC Address. The value might be specified as a number between 0 and 65535. The factory default is 32768.
STP Statistics	
Topology Change Count	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
Time Since Topology Changed	Time (in days, hours, minutes, and seconds) since a topology change was detected by the bridge.
Designated Root	The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
Root Cost	The cost of the path to the root as seen from this bridge.

Table 5-4 Spanning Tree Protocol Fields Page Fields (continued)

Field	Description
Root Port	The port number of the port which offers the lowest cost path from this bridge to the root bridge.
Maximum Age (seconds)	The value that all bridges use for MaxAge when this bridge is acting as the root. **Note** The 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Hello Time. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 6 through 40 seconds. The factory default is 20.
Hello Time (seconds)	The value that all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by 802.1D-1990 to be 1 second. Valid values are 1 through 10 seconds. The factory default is 2.
Forward Delay (seconds)	The value that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1990 specifies that the range for this parameter is related to the value of Stp Bridge Maximum Age. The granularity of this timer is specified by 802.1D-1990 to be 1 second. An agent might return a badValue error if a set is attempted to a value which is not a whole number of seconds. Valid values are 4 through 30 seconds. The factory default is 15.
Hold Time (seconds)	The minimum time period to elapse between the transmission of Configuration BPDUs through a given LAN Port: at most one Configuration BPDU shall be transmitted in any Hold Time period.

Monitoring CLI Sessions

The CLI Sessions page for a controller can be accessed in the following ways:

- Choose **Monitor > Controllers**, click the applicable IP address, then choose **System > CLI Sessions** from the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **System > CLI Sessions** from the left sidebar menu.

Table 5-5 lists CLI Sessions page fields.

Table 5-5 CLI Sessions Page Fields

Field	Description
Session Index	Session identification.
Username	Login username.
Connection Type	Telnet or serial session.
Connection From	IP address of the client computer system.
Session Time	Elapsed active session time.
Idle Time	Elapsed inactive session time.

Monitoring DHCP Statistics

The NCS provides DHCP server statistics for Version 5.0.6.0 controllers or later. These statistics include information on the packets sent and received, DHCP server response information, and the last request time stamp.

To access this page, choose **Monitor > Controllers**, click the applicable IP address, then choose **System > DHCP Statistics** from the left sidebar menu.

Table 5-6 lists the The DHCP Statistics page fields.

Table 5-6 DHCP Statistics Page Fields

Field	Description
Server IP	Identifies the IP address of the server.
Is Proxy	Identifies whether or not this server is proxy.
Discover Packets Sent	Identifies the total number of packets sent intended to locate available servers.
Request Packets Sent	Identifies the total number of packets sent from the client requesting parameters from the server or confirming the correctness of an address.
Decline Packets	Identifies the number of packets indicating that the network address is already in use.
Inform Packets	Identifies the number of client requests to the DHCP server for local configuration parameters because the client already has an externally configured network address.
Release Packets	Identifies the number of packets that release the network address and cancel the remaining lease.
Reply Packets	Identifies the number of reply packets.
Offer Packets	Identifies the number of packets that respond to the discover packets with an offer of configuration parameters.
Ack Packets	Identifies the number of packets that acknowledge successful transmission.
Nak Packets	Identifies the number of packets that indicate that the transmission occurred with errors.
Tx Failures	Identifies the number of transfer failures that occurred.
Last Response Received	Provides a timestamp of the last response received.
Last Request Sent	Provides a timestamp of the last request sent.

Monitoring WLANs

Choose **Monitor > Controllers** click a controller IP address, and choose **WLANs** from the left sidebar menu. This page enables you to view a summary of the wireless local access networks (WLANs) that you have configured on this controller.

Table 5-7 lists the WLAN Details page fields.

Table 5-7 WLAN Page Fields

Field	Description
WLAN ID	Identification number of the WLAN.
Profile Name	User-defined profile name specified when initially creating the WLAN. Profile Name is the WLAN name.
SSID	User-defined SSID name.
Security Policies	Security policies enabled on the WLAN.
No of Mobility Anchors	Mobility anchors are a subset of a mobility group specified as the anchor controllers for a WLAN.
Admin Status	Status of the WLAN is either enabled or disabled.
No. of Clients	Current number of clients currently associated with this WLAN.

Monitoring Ports

This section provides the detailed information regarding monitoring controller port parameters and contains the following topics:

Monitoring General Ports

The Ports > General page provides information regarding physical ports on the selected controller. Click a port number to view details for that port. See the "Port Details" section on page 5-10 for more information.

Table 5-8 lists the General page fields.

Table 5-8 General Page Fields

Field	Description
Port	Click the port number to view port details. See the "Port Details" section on page 5-10 for more information.
Physical Mode	Displays the physical mode of all ports. The choices include the following: – 100 Mbps Full Duplex – 100 Mbps Half Duplex – 10 Mbps Full Duplex – 10 Mbps Half Duplex
Admin Status	Displays the port state as either Enable or Disable.
STP State	Displays the STP state of the port as either Forwarding or Disabled.
Physical Status	Displays the actual port physical interface: – Auto Negotiate – Half Duplex 10 Mbps – Full Duplex 10 Mbps – Half Duplex 100 Mbps – Full Duplex 100 Mbps – Full Duplex 1 Gbps
Link Status	Red (down/failure), Yellow (alarm), Green (up/normal).

To access the Monitor > Ports > General page, do one of the following:

- Choose **Configure > Controllers**, click the applicable IP address. From the left sidebar menu, choose **General** under Ports.
- Choose **Monitor > Controllers**, click the applicable, and click a port to access this page.
- Choose **Monitor > Access Points** and click a list item under AP Name, click **Registered Controller**, then click a port to access this page.
- Choose **Monitor > Clients** and click a list item under AP Name, then click **Registered Controller**, then click a port to access this page.

Port Details

Note Click **Alarms** to open the Monitor Alarms page. See the "Monitoring Alarms" section on page 5-131 for more information.
Click Events to open the Monitor Events page. See the "Monitoring Events" section on page 5-149 for more information.

Table 5-9 lists the Port Detail page fields.

Table 5-9 Port Details Page Fields

Field	Description
Interface	
Operational Status	Displays the operational status of the controller: The options are UP or DOWN.
Unknown Protocol Packets	The number of packets of unknown type which were received from this server on this port.
Traffic (Received and Transmitted)	
Total Bytes	The total number of packets received.
Packets	The total number of packets (including bad packets) received that were within the indicated octet range in length (excluding framing bits but including FCS octets). Ranges include the following: – 64 Octets – 65-127 Octets – 128-255 Octets – 256-511 Octets – 512-1023 Octets – 1024-1518 Octets
Packets (Received and Transmitted)	
Total	Total number of packets received/transmitted.
Unicast Packets	The number of subnetwork-unicast packets delivered/sent to a higher-layer protocol.
Broadcast Packets	The total number of packets received/sent that were directed to the broadcast address.
Packets Discarded	Packets Discarded (Received/Transmitted): The number of inbound/outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Errors in Packets	The total number of packets received with errors.
Received packets with MAC errors	

Table 5-9 Port Details Page Fields (continued)

Field	Description
Jabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). **Note** This definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10Base-5) and section 10.3.1.4 (10Base-2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 and 150 ms.
Fragments/Undersize	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
Alignment Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
FCS Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.
Transmit discards	
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Deferred Transmissions	A count of frames for which transmission on a particular interface fails due to deferred transmissions.
Late Collisions	A count of frames for which transmission on a particular interface fails due to late collisions.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
Ether Stats	

Table 5-9 Port Details Page Fields (continued)

Field	Description
CRC Align Errors	The number of incoming packets with the Checksum (FCS) alignment error. This represents a count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
Undersize Packets	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
Oversize Packets	The total number of frames that exceeded the maximum permitted frame size. This counter has a maximum increment rate of 815 counts per second at 10 Mbps.
Ether Stats Collisions	The number of packets with collision errors.
SQE Test Errors	Signal Quality Error Test errors (that is, Heartbeat) during transmission. This tests the important collision detection electronics of the transceiver, and lets the Ethernet interface in the computer know that the collision detection circuits and signal paths are working correctly. The errors indicate a count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLong property, the AlignmentErrors property, or the FCSErrors property. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object might represent a count of receive errors on a particular interface that are not otherwise counted.

Table 5-9 Port Details Page Fields (continued)

Field	Description
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions property, the ExcessiveCollisions property, or the CarrierSenseErrors property. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object might represent a count of transmission errors on a particular interface that are not otherwise counted.
Carrier Sense Errors	The Carrier Sense detects the presence of a carrier. The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface.
Too Long Frames	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the FrameTooLong status is returned by the MAC layer to the LLC (or other MAC user). Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

Monitoring CDP Interface Neighbors

To access the Monitor CDP Interface Neighbors page, follow these steps:

Step 1 Choose **Monitor > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **CDP Interface Neighbors** (under the Port heading).

Step 4 Table 5-10 lists the CDP Interface Neighbors page fields.

Table 5-10 CDP Interface Neighbors Page Fields

Field	Description
Local Interface	Local Port information.
Neighbor Name	The name of each CDP neighbor.
Neighbor Address	The IP address of each CDP neighbor.
Neighbor Port	The port used by each CDP neighbor for transmitting CDP packets.
Capability	The functional capability of each CDP neighbor.
Platform	The hardware platform of each CDP neighbor device.
Duplex	Indicates Full Duplex or Half Duplex.
Software Version	The software running on the CDP neighbor.

Monitoring Controller Security

This section provides the detailed information regarding monitoring controller security and contains the following topics:

Monitoring RADIUS Authentication

The RADIUS Authentication page displays RADIUS authentication server information and enables you to add or delete a RADIUS authentication server.

To access this page, do one of the following:

- Choose **Monitor > Controllers**, click the applicable IP address, then choose **Security > Radius Authentication** from the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **Security > Radius Authentication** from the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **Security > Radius Authentication** from the left sidebar menu.

Table 5-11 lists the RADIUS Authentication page fields.

Table 5-11 RADIUS Authentictaion Page Fields

Field	Description
RADIUS Authentication Servers	
Server Index	Access priority number for RADIUS servers. Up to four servers can be configured, and controller polling of the servers starts with Index 1, Index 2 second, and so forth. The index number is based on when the RADIUS server is added to the controller.
IP Address	The IP address of the RADIUS server.
Ping	Click the icon to ping the RADIUS server from the controller to verify the link.
Port	Controller port number for the interface protocols.
Admin Status	Indicates whether the server is enabled or disabled.
Authentication Server Statistics	
Msg Round Trip Time	The time interval (in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
First Requests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
Retry Requests	The number of RADIUS Authentication-Request packets retransmitted to this RADIUS authentication server.
Accept Responses	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
Reject Responses	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
Challenge Responses	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
Malformed Msgs	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or unknown types are not included as malformed access responses.

Table 5-11 RADIUS Authentictaion Page Fields (continued)

Field	Description
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout, or retransmission.
Bad Authentication Msgs	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
Timeouts Requests	The number of authentication timeouts to this server. After a timeout the client might retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Unknown Type Msgs	The number of RADIUS packets of unknown type which were received from this server on the authentication port.
Other Drops	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

Monitoring RADIUS Accounting

You can access this page by any of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address, then choose **Security > Radius Accounting** from the left sidebar menu.
- Choose **Monitor > Clients** and click a list item under AP Name, click **Registered Controller**, then choose **Security > Radius Accounting** from the left sidebar menu.
- Choose **Monitor > Maps**, click an item in the **Name** column, click an access point icon, click **Controller**, then choose **Security > Radius Accounting** from the left sidebar menu.
- Choose **Configure > Access Points** and select a list item under AP Name, click **Registered Controller**, then choose **Security > Radius Accounting** from the left sidebar menu.

Table 5-12 lists the RADIUS Accounting page fields.

Table 5-12 RADIUS Accoungting Page Fields

Field	Description
RADIUS Accounting Server	
Server Index	Access priority number for RADIUS servers. Up to four servers can be configured, and controller polling of the servers starts with Index 1, Index 2 second, and so forth. Index number is based on when the RADIUS server is added to the controller.
IP Address	The IP address of the RADIUS server.
Ping	Click the icon to ping the RADIUS Server from the controller to verify the link.
Port	The port of the RADIUS server.
Admin Status	Indicates whether the server is enabled or disabled.
Accounting Statistics	
Msg Round Trip Time	The time interval (in milliseconds) between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
First Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Retry Requests	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Accounting Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Msgs	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authentication Msgs	The number of RADIUS Accounting-Response packets which contained invalid authenticators received from this server.

Table 5-12 RADIUS Accoungting Page Fields (continued)

Field	Description
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Timeouts Requests	The number of accounting timeouts to this server. After a timeout the client might retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
Unknown Type Msgs	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
Other Drops	The number of RADIUS packets which were received from this server on the accounting port and dropped for some other reason.

Monitoring Management Frame Protection

This page displays the Management Frame Protection (MFP) summary information. MFP provides the authentication of 802.11 management frames. Management frames can be protected to detect adversaries who are invoking denial of service attacks, flooding the network with probes, interjecting as rogue access points, and affecting the network performance by attacking the QoS and radio measurement frames.

If one or more of the WLANs for the controller has MFP enabled, the controller sends each registered access point a unique key for each BSSID the access point uses for those WLANs. Management frames sent by the access point over the MFP enabled WLANs is signed with a Frame Protection Information Element (IE). Any attempt to alter the frame invalidates the message causing the receiving access point configured to detect MFP frames to report the discrepancy to the WLAN controller.

Access this page in one of the following ways:

- Choose **Monitor > Controllers**. From the Controllers > Search Results page, click the applicable IP address, then choose **Security > Management Frame Protection** from the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **Security > Management Frame Protection** from the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **Security > Management Frame Protection** from the left sidebar menu.

Table 5-13 lists the MFP page fields.

Table 5-13 MFP Page Fields

Field	Description
General	
Management Frame Protection	Indicates if the infrastructure MFP is enabled globally for the controller.
Controller Time Source Valid	The Controller Time Source Valid field indicates whether the controller time is set locally (by manually entering the time) or through an external source (such as NTP server). If the time is set by an external source, the value of this field is "True." If the time is set locally, the value is "False." The time source is used for validating the timestamp on management frames between access points of different controllers within a mobility group.
WLAN Details	
WLAN ID	The WLAN ID, 1 through 17.
WLAN Name	User-defined profile name when initially creating the WLAN. Both the SSID name and profile name are user-defined. The WLAN name is same as the profile name.
MFP Protection	Management Frame Protection is either enabled or disabled.
Status	Status of the WLAN is either enabled or disabled.
AP Details	
AP Name	Operator-defined name of access point.
MFP Validation	Management Frame Protection is enabled or disabled.
Radio	802.11a or 802.11b/g.
Operation Status	Displays the operational status: either UP or DOWN.
Protection	Full (All Frames).
Validation	Full (All Frames).

Monitoring Rogue AP Rules

Rogue AP rules automatically classify rogue access points based on criteria such as authentication type, matching configured SSIDs, client count, and RSSI values. The NCS applies the rogue access point classification rules to the controllers and respective access points.

These rules can limit a rogue appearance on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

Rogue AP Rules also help reduce false alarms.

Note Rogue classes include the following types:
Malicious Rogue—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly AP category.
Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.
Unclassified Rogue—A detected access point that does not match the malicious or friendly rules.

Choose **Monitor > Controllers**. From the Controllers > Search Results page, click the applicable IP address, then choose **Security > Rogue AP Rules** from the left sidebar menu.

The **Rogue AP Rules** page provides a list of all rogue access point rules currently applied to this controller.

The following information is displayed for rogue access point rules:

- Rogue AP Rule name—Click the link to view Rogue AP Rule details.
- Rule Type—Malicious or Friendly.
  - Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category.
  - Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.
- Priority—Indicates the priority level for this rogue AP rule.

Note See the "Configuring a Rogue AP Rules Template" section on page 10-83 for more information on Rogue AP Rules.

Rogue AP Rules

Table 5-14 lists the Rogue AP Rules page fields.

Table 5-14 Rogue AP Rule Page Fields

Field	Description
Rule Name	Name of the rule.
Rule Type	Malicious or Friendly – Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category. – Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.

Table 5-14 Rogue AP Rule Page Fields (continued)

Field	Description
Match Type	Match any or match all conditions.
Enabled Rule Conditions	Indicates all enabled rule conditions including: – Open Authentication – Match Managed AP SSID – Match User Configured SSID – Minimum RSSI – Time Duration – Minimum Number Rogue Clients

Note See the "Configuring a Rogue AP Rules Template" section on page 10-83 for more information on Rogue AP Rules.

Monitoring Guest Users

Choose **Monitor > Controllers**. From the Controllers > Search Results page, click the applicable IP Address, then choose **Security > Guest Users** from the left sidebar menu.

The NCS allows you to monitor guest users from the Guest Users page as well as from the NCS home page.

The Guest Users page provides a summary of the guest access deployment and network use.

The following information is displayed for guest users currently associates on the network. Table 5-15 lists the Guest Users page fields.

Table 5-15 Guest Users Page Fields

Field	Description
Guest User Name	Indicates the guest user login name.
Profile	Indicates the profile to which the guest user is connected.
Lifetime	Indicates the length of time that the guest user account is active. Length of time appears in days, hours, and minutes or as Never Expires.
Start Time	Indicates when the guest user account was activated.
Remaining Lifetime	Indicates the remaining time for the guest user account.
Role	Indicates the designated user role.
First Logged in at	Indicates the date and time of the user first login.

Table 5-15 Guest Users Page Fields (continued)

Field	Description
Number of logins	Indicates the total number of logins for this guest user.
Description	User-defined description of the guest user account for identification purposes.

Monitoring Controllers Mobility

Monitoring Mobility Stats

The Mobility Stats page displays the statistics for mobility group events.

Access this page in one of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address, then choose **Mobility > Mobility Stats** from the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **Mobility > Mobility Stats** from the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **Mobility > Mobility Stats** from the left sidebar menu.

Table 5-16 lists the Mobility Stats page fields.

Table 5-16 Mobility Stats Page Fields

Field	Description
Global Mobility Statistics	
Rx Errors	Generic protocol packet receive errors, such as packet too short or format incorrect.
Tx Errors	Generic protocol packet transmit errors, such as packet transmission fail.
Responses Retransmitted	The Mobility protocol uses UDP and it resends requests several times if it does not receive a response. Because of network or processing delays, the responder might receive one or more retry requests after it initially responds to a request. This is a count of the response resends.
Handoff Requests Received	Total number of handoff requests received, ignored or responded to.
Handoff End Requests	Total number of handoff end requests received. These are sent by the Anchor or the Foreign to notify the other about the close of a client session.
State Transitions Disallowed	PEM (policy enforcement module) has denied a client state transition, usually resulting in the handoff being aborted.

Table 5-16 Mobility Stats Page Fields (continued)

Field	Description
Resource Unavailable	A necessary resource, such as a buffer, was unavailable, resulting in the handoff being aborted.
Mobility Responder Statistics	
Handoff Requests Ignored	Number of handoff requests/client announces that were ignored. The controller simply had no knowledge of that client.
Ping Pong Handoff Requests Dropped	Number of handoff requests that were denied because the handoff period was too short (3 sec).
Handoff Requests Dropped	Number of handoff requests that were dropped due to a either an incomplete knowledge of the client or a problem with the packet.
Handoff Requests Denied	Number of handoff requests that were actively denied.
Client Handoff as Local	Number of handoffs responses sent while in the local role.
Client Handoff as Foreign	Number of handoffs responses sent while in the foreign role.
Anchor Requests Received	Number of anchor requests received.
Anchor Requests Denied	Number of anchor requests denied.
Anchor Requests Granted	Number of anchor requests granted.
Anchor Transferred	Number of anchors transferred because the client has moved from a foreign controller to controller on the same subnet as the current anchor.
Mobility Initiator Statistics	
Handoff Requests Sent	Number of clients that have associated with controller and have been announced to the mobility group.
Handoff Replies Received	Number of handoff replies that have been received in response to the requests sent.
Handoff as Local Received	Number of handoffs in which the entire client session has been transferred.
Handoff as Foreign Received	Number of handoffs in which the client session was anchored elsewhere.
Handoff Denies Received	Number of handoffs that were denied.
Anchor Request Sent	Number of anchor requests that were sent for a three party (foreign to foreign) handoff. Handoff was received from another foreign and the new controller is requesting the anchor to move the client.
Anchor Deny Received	Number of anchor requests that were denied by the current anchor.

Table 5-16 Mobility Stats Page Fields (continued)

Field	Description
Anchor Grant Received	Number of anchor requests that were approved by the current anchor.
Anchor Transfer Received	Number of anchor transfers that were received by the current anchor.

Monitoring Controller 802.11a/n

This section provides detailed information regarding monitoring 802.11a/n parameters and contains the following topics:

Monitoring 802.11a/n Parameters

Access the 802.11a/n Parameters page in one of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address, then choose **Parameters** from the 802.11a/n section of the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **Parameters** from the 802.11a/n section of the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **Parameters** from the 802.11a/n section of the left sidebar menu.

Table 5-17 lists the 802.11a/n Parameters page fields.

Table 5-17 802.11 a/n Parameters Page Fields

Field	Description
MAC Operation Parameters	
RTS Threshold	Indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed. **Note** An RTS/CTS handshake is performed at the beginning of any frame exchange sequence where the MPDU is a data or management type, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute higher than the maximum MSDU size turns off the RTS/CTS handshake for data or management type frames transmitted by this STA. Setting this attribute to zero turns on the RTS/CTS handshake for all transmitted data or management type frames.

Table 5-17 802.11 a/n Parameters Page Fields (continued)

Field	Description
Short Retry Limit	The maximum number of transmission attempts of a frame (less than or equal to dot11RTSThreshold) made before a failure condition is indicated. The default value is 7.
Long Retry Limit	The maximum number of transmission attempts of a frame (greater than dot11RTSThreshold) made before a failure condition is indicated. The default value is 4.
Max Tx MSDU Lifetime	The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU are terminated. The default value is 512.
Max Rx Lifetime	The elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU are terminated. The default value is 512.
Physical Channel Fields	
TI Threshold	The threshold being used to detect a busy medium (frequency). CCA shall report a busy medium upon detecting the RSSI above this threshold.
Channel Agility Enabled	Physical channel agility functionality is or is not implemented.
Station Configuration Fields	
Medium Occupancy Limit	Indicates the maximum amount of time, in TU, that a point coordinator might control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
CFP Period	The number of DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.
CFP Max Duration	The maximum duration of the CFP in TU that might be generated by the PCF. It is modified by MLME-START.request primitive.
CF Pollable	When this attribute is implemented, it indicates that the client is able to respond to a CF-Poll with a data frame within a SIFS time. This attribute is not implemented if the STA is not able to respond to a CF-Poll with a data frame within a SIFS time.

Table 5-17 802.11 a/n Parameters Page Fields (continued)

Field	Description
CF Poll Request	Specifies whether CFP is requested by the client.
DTIM Period	The number of beacon intervals that elapse between transmission of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.

Monitoring 802.11a/n RRM Groups

Access the RRM Grouping page in one of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address, then choose **Grouping** or **WPS Grouping** from the 802.11a/n section of the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **RRM Grouping** or **WPS Grouping** from the 802.11a/n section of the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **RRM Grouping** or **WPS Grouping** from the 802.11a/n section of the left sidebar menu.

Table 5-18 lists the 802.11a/n RRM Grouping page fields.

Table 5-18 802.11 a/n RRM Grouping Page Fields

Field	Description
802.11a Grouping Control	
Grouping Mode	Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs. Each controller optimizes only its own parameters of the access point. When grouping is on, the controller forms groups and elects leaders to perform better dynamic parameter optimization.

Table 5-18 802.11 a/n RRM Grouping Page Fields (continued)

Field	Description
Grouping Role	There are five grouping roles: – None—This grouping role appears when the RF Group Mode is configured as Off. – Auto-Leader—This grouping role appears when the RF Group Mode is configured as Automatic and the controller is elected as a leader by the automatic grouping algorithm. – Auto-Member—This grouping role appears when the RF Group Mode is configured as Automatic and the controller is selected as a member by the automatic grouping algorithm. – Static-Leader—This grouping role appears when the RF Group Mode is configured as Leader. – Static-member—This grouping role appears when the RF Group Mode is configured as automatic and the controller joins the leader as a result of the join request from the leader.
Group Leader IP Address	This is the IP address of the group leader.
Group Leader MAC Address	This is the MAC address of the group leader for the group containing this controller.
Is 802.11a Group Leader	Yes, if this controller is the group leader or No if the controller is not the group leader.
Last Update Time (secs)	The elapsed time since the last group update in seconds. This is only valid if this controller is a group leader.
Group Update Interval (secs)	When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 3600 seconds.
Group Members	
Group Member Name	Name of group member(s).
Group Member IP Address	IP address of group member(s).
Member Join Reason	Current state of the member(s).

Monitoring Controllers 802.11b/g/n

This section provides the detailed information regarding monitoring 802.11b/g/n parameters and contains the following topics:

Monitoring 802.11b/g/n Parameters

Access the 802.11b/g/n Parameters page in one of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP Address, then choose **Parameters** from the 802.11b/g/n section of the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **Parameters** from the 802.11b/g/n section of the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **Parameters** from the 802.11b/g/n section of the left sidebar menu.

Table 5-19 lists the 802.11b/g Parameters page fields.

Table 5-19 802.11 b/g/n Parameters Page Fields

Field	Description
MAC Operation Parameters	
RTS Threshold	Indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed. **Note** An RTS/CTS handshake is performed at the beginning of any frame exchange sequence where the MPDU is a data or management type, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute higher than the maximum MSDU size turns off the RTS/CTS handshake for data or management type frames transmitted by this STA. Setting this attribute to zero turns on the RTS/CTS handshake for all transmitted data or management type frames.
Short Retry Limit	The maximum number of transmission attempts of a frame (less than or equal to dot11RTSThreshold) made before a failure condition is indicated. The default value is 7.
Long Retry Limit	The maximum number of transmission attempts of a frame (greater than dot11RTSThreshold) made before a failure condition is indicated. The default value is 4.

Table 5-19 802.11 b/g/n Parameters Page Fields (continued)

Field	Description
Max Tx MSDU Lifetime	The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU are terminated. The default value is 512.
Max Rx Lifetime	The elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU are terminated. The default value is 512.
Physical Channel Fields	
TI Threshold	The threshold being used to detect a busy medium (frequency). CCA shall report a busy medium upon detecting the RSSI above this threshold.
Channel Agility Enabled	Physical channel agility functionality is or is not implemented.
Station Configuration Fields	
Medium Occupancy Limit	Indicates the maximum amount of time, in TU, that a point coordinator might control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
CFP Period	The number of DTIM intervals between the start of CFPs. It is modified by MLME-START.request primitive.
CFP Max Duration	The maximum duration of the CFP in TU that might be generated by the PCF. It is modified by MLME-START.request primitive.
CF Pollable	When this attribute is implemented, it indicates that the client is able to respond to a CF-Poll with a data frame within a SIFS time. This attribute is not implemented if the STA is not able to respond to a CF-Poll with a data frame within a SIFS time.
CF Poll Request	Specifies whether CFP is requested by the client.
DTIM Period	The number of beacon intervals that elapse between transmission of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.

Monitoring 802.11b/g/n RRM Groups

Access the 802.11b/g/n RRM Grouping page in one of the following ways:

- Choose **Monitor > Controllers** and click the applicable IP address, then choose **RRM Grouping** or **WPS Grouping** from the 802.11b/g/n section of the left sidebar menu.

- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **RRM Grouping** or **WPS Grouping** from the 802.11b/g/n section of the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **RRM Grouping** or **WPS Grouping** from the 802.11b/g/n section of the left sidebar menu.

Table 5-20 lists the 802.11b/g/n RRM grouping page fields.

Table 5-20 802.11 b/g/n RRM Grouping Page Fields

Field	Description
802.11 b/g/n Grouping Control	
Grouping Mode	Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs. Each controller optimizes only its own parameters of the access point. When grouping is on, the controller forms groups and elects leaders to perform better dynamic parameter optimization.
Grouping Role	There are five grouping roles: – None—This grouping role appears when the RF Group Mode is configured as Off. – Auto-Leader—This grouping role appears when the RF Group Mode is configured as Automatic and the controller is elected as a leader by the automatic grouping algorithm. – Auto-Member—This grouping role appears when the RF Group Mode is configured as Automatic and the controller is selected as a member by the automatic grouping algorithm. – Static-Leader—This grouping role appears when the RF Group Mode is configured as Leader. – Static-member—This grouping role appears when the RF Group Mode is configured as automatic and the controller joins the leader as a result of the join request from the leader.
Group Leader IP Address	This is the IP address of the group leader.
Group Leader MAC Address	This is the MAC address of the group leader for the group containing this controller.
Is 802.11a Group Leader	Yes, if this controller is the group leader or No if the controller is not the group leader.
Last Update Time (secs)	The elapsed time since the last group update in seconds. This is only valid if this controller is a group leader.

Table 5-20 802.11 b/g/n RRM Grouping Page Fields (continued)

Field	Description
Group Update Interval (secs)	When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 3600 seconds.
Group Members	
Group Member Name	Name of group member(s).
Group Member IP Address	IP address of group member(s).
Member Join Reason	Current state of the member(s).

Monitoring Controllers IPv6

Monitoring Neighbor Bind Counter Statistics

Access the Neighbor Bind Counter Statistics page in one of the following ways:

- Choose **Monitor > Controllers**, select an IP Address, and choose **IPv6 > Neighbor Bind Counters** from the left sidebar menu.
- Choose **Monitor > Access Points**, click a list item under AP Name, click **Registered Controller**, then choose **IPv6 > Neighbor Bind Counters** from the left sidebar menu.
- Choose **Monitor > Clients**, click a list item under AP Name, click **Registered Controller**, then choose **IPv6 > Neighbor Bind Counters** from the left sidebar menu.

Table 5-21 lists the Neighbor Bind Counter Stats page fields.

Table 5-21 Neighbor Bind Counter Stats Page Fields

Field	Description
Neighbor Bind Counters	Provides the statistics of the number of messages exchanged between the host or client and the router to generate and acquire IPv6 addresses, link, MTU, and so on.
Received Messages	The number of Advertisement, Solicitation and other messages received for NDP and DHCPv6.
Bridged Messages	The number of Advertisement, Solicitation and other messages bridged for NDP and DHCPv6.
Total Snooping Dropped Messages	The number of Advertisement, Solicitation and other messages bridged for NDP and DHCPv6 along with the reason for the drop.

Table 5-21 Neighbor Bind Counter Stats Page Fields (continued)

Field	Description
Neighbor Discovery Suppress Drop Counter	The total number of neighbor discovery messages dropped.
Total Suppress Dropped Messages	The reason for the neighbor discovery messages drop.

Note Hover your mouse cursor over the values in the Total Snooping/Suppress Drop Messages column to see the reasons due to which the corresponding messages were dropped.

Monitoring Switches

Choose **Monitor > Switches** to view the detailed information about the switches. This section provides more detailed information regarding monitoring switches and includes the following topics:

- Searching Switches, page 5-33
- Viewing the Switches, page 5-34
- Monitoring Switch System Parameters, page 5-34
- Monitoring Switch Interfaces, page 5-40
- Monitoring Switch Clients, page 5-42

Searching Switches

Use the NCS search feature to find specific switches or to create and save custom searches.

You can configure the following fields when performing an advanced search for switches (see Table 5-22).

Table 5-22 Search Switches Fields

Field	Options
Search for Switches by	Choose **All Switches**, **IP Address**, or **Switch Name**. You can use wildcards (*). For example, if you select IP Address and enter 172*, the NCS returns all switches that begin with IP address 172.
Items per page	Select the number of switches to return per page.

See one of the following topics for additional information:

- Using the Search Feature, page 2-33
- Quick Search, page 2-33
- Advanced Search, page 2-34
- Saved Searches, page 2-46

Viewing the Switches

Choose **Monitor > Switches** to view a list of the switches. From this page you can view a summary of the switches including the default information shown in Table 5-23.

Table 5-23 Viewing the Switches

Field	Description
IP Address	The IP address assigned to the switch. Click a list item to view access point details.
Device Name	Name of the switch.
Device Type	Type of switch.
Reachability Status	Indicates OK if the switch is reachable or Unreachable if the switch is not reachable.
Endpoint Count	Number of endpoints on the switch.

Configuring the Switch List Page

The Edit View page allows you to add, remove, or reorder columns in the Switches table.

To edit the available columns in the table, follow these steps:

Step 1 Choose **Monitor > Switches**.

Step 2 Click the **Edit View** link.

Step 3 To add an additional column to the table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the table.

Step 4 To remove a column from the table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. All items in the left column are not displayed in the table.

Step 5 Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.

Step 6 Click **Reset** to restore the default view.

Step 7 Click **Submit** to confirm the changes.

Monitoring Switch System Parameters

Choose **Monitor > Switches**, then click an IP address in the IP Address column to view details about the switch. This section provides the detailed information regarding each switch details page and contains the following topics:

- Viewing Switch Summary Information, page 5-35
- Viewing Switch Memory Information, page 5-36
- Viewing Switch Environment Information, page 5-36
- Viewing Switch Module Information, page 5-37
- Viewing Switch VLAN Information, page 5-37

Viewing Switch Summary Information

Choose **Monitor > Switches**, then click an IP address in the IP Address column to view details about the switch. Table 5-24 describes the summary information that is displayed.

Table 5-24 Viewing Switches Summary Information

General	
IP Address	IP address of the switch.
Device Name	Name of the switch.
Device Type	Switch type.
Up Time	Time since last reboot.
System Time	Time on the switch.
Reachability Status	which can be the following: • Reachable • Unreachable
Location	Location of the switch.
Contact	Contact name for the switch.
Cisco Identity Capable	Specifies if the switch is identity-capable.
Location Capable	Specifies if the switch is capable of storing the location information.
CPU Utilization	Displays a graph of the maximum, average, and minimum CPU utilization over the specified amount of time.
Unique Device Identifier (UDI)	
Name	Product type.
Description	Description of UDI.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial Number	Unique product serial number.
Inventory	
Software Version	Version of software currently running on the switch.
Model No.	Model number of the switch.
Port Summary	
Number of Ports Up	Number of ports up on the switch.

Table 5-24 Viewing Switches Summary Information (continued)

Number of Ports Down	Number of ports down on the switch.
Memory Utilization	Displays a graph of the maximum, average, and minimum memory utilization over the specified amount of time.

Related Topic

- Monitoring Switch Interfaces, page 5-40

Viewing Switch Memory Information

Choose **Monitor > Switches**, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose **Memory**. Table 5-25 describes the memory information that is displayed.

Table 5-25 Viewing Switches Memory Information

Memory Pool	
Type	Type of memory.
Name	Name assigned to the memory pool.
Used (MB)	Amount of memory (in MB) used.
Free (MB)	Amount of memory (in MB) available.

Viewing Switch Environment Information

Choose **Monitor > Switches**, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose **Environment**. Table 5-26 describes the environment information that is displayed.

Table 5-26 Viewing Switches Environment Information

Power Supply	
Model Name	Model name of the power supply.
Description	Description of the power supply.
Operational Status	Status of the associated power supply: • Green—Power supply is operational. • Red—Power supply is inoperable.
Manufacturer Name	Name of the power supply manufacturer.
Free	Free power supply slots.
Vendor Equipment Type	Description of vendor equipment type.
Fans	
Name	Name of fan.
Description	Description of fan.

Table 5-26 Viewing Switches Environment Information (continued)

Operational Status	Status of the fan: • Green—Fan is operational. • Red—Fan is inoperable.
Vendor Equipment Type	Description of vendor equipment type.
Serial Number	Serial number of the fan.

Viewing Switch Module Information

Choose **Monitor > Switches**, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose **Modules**. Table 5-27 describes the module information that is displayed.

Table 5-27 Viewing Switches Modules Information

Modules	
Product Name	Name of the module.
Physical Location	Location where the module is contained.
Number of Ports	Number of ports supported by the module.
Operational State	Operational status of the module.
Equipment Type	Type of equipment.
Inline Power Capable	Specifies whether the module has inline power capability.

Viewing Switch VLAN Information

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose **VLANs**. Table 5-28 describes the VLAN information that is displayed.

Table 5-28 Viewing Switches VLANs Information

VLANs	
VLAN ID	ID of the VLAN.
VLAN Name	Name of the VLAN.
VLAN Type	Type of VLAN.

Viewing Switch VTP Information

Choose **Monitor > Switches**, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose **VTP**. Table 5-29 describes the VTP information that is displayed.

Table 5-29 Viewing Switches VTP Information

VTP	
VTP Domain Name	Name of the VTP domain.
VTP Version	Version of VTP in use.
VTP Mode	The VTP mode: • Client • Server • Transparent—Does not generate or listen to VTP messages, but forwards messages. • Off—Does not generate, listen to, or forward any VTP messages.
Pruning Enabled	Specifies whether VTP pruning is enabled.

Viewing Switch Physical Ports Information

Choose **Monitor > Switches**, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose **Physical Ports**. Table 5-30 describes the physical ports information that is displayed.

Table 5-30 Viewing Switches Physical Ports Information

Physical Ports	
Port Name	Name of the physical port.
Port Description	Description of the physical port.
Residing Module	Module on which the physical port resides.
Vendor Equipment Type	Description of vendor equipment type.

Viewing Switch Sensor Information

Choose **Monitor > Switches**, then click an IP address under the IP Address column to view details about the switch. From the System menu, choose **Sensors**. Table 5-31 describes the sensor information that is displayed.

Table 5-31 Viewing Switches Sensors Information

Sensors	
Sensor Name	Name of the sensor.
Sensor Description	Description of the sensor.
Type	Type of sensor.
Vendor Sensor Type	Description of vendor sensor type.
Equipment Name	Name of equipment.

Table 5-31 Viewing Switches Sensors Information (continued)

Precision	When in the range 1 to 9, precision is the number of decimal places in the fractional part of a Sensor Value fixed-point number. When in the range -8 to -1, Sensor Precision is the number of accurate digits in a SensorValue fixed-point number.
Status	Operational status of the sensor.

Viewing Switch Spanning Tree Information

Choose **Monitor > Switches**, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose **Spanning Tree**. Table 5-32 describes the spanning tree information that is displayed.

Table 5-32 Viewing Switches Spanning Tree Information

Spanning Tree	
STP Instance ID	ID of the STP. Click an STP Instance ID to see the spanning tree details as described in the "Viewing Spanning Tree Details" section on page 5-39.
VLAN ID	ID of the VLAN.
Root Path Cost	Root cost of the path.
Designated Root	Forwarding port.
Bridge Priority	Priority of the bridge.
Root Bridge Priority	Priority number of the root bridge.
Max Age (sec)	STP timer value for maximum age (in seconds).
Hello Interval (sec)	STP timer value (in seconds).

Viewing Spanning Tree Details

Choose **Monitor > Switches**, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose **Spanning Tree**, then click an STP instance ID to see the spanning tree details as described in Table 5-33.

Table 5-33 Viewing Spanning Tree Details

Spanning Tree	
STP Port	Name of the STP port.
Port Role	Role of the port.
Port Priority	Priority number of the port.
Path Cost	Cost of the path.
Port State	State of the port.
Port Type	Type of port.

Viewing Switch Stacks Information

Choose **Monitor > Switches**, then click an IP address in the IP Address column to view details about the switch. From the System menu, choose **Stacks**. Table 5-34 describes the spanning tree information that is displayed.

Table 5-34 Viewing Switches Stacks Information

Stacks	
MAC Address	MAC address of the stack.
Role	Role of the stack: • Master—Stack master • Member—Active member of the stack • Not Member—Non-active stack member
Switch Priority	Priority number of the switch.
State	Current state of the stack.
Software Version	Software image running on the switch.

Viewing Switch NMSP and Location Information

You can view the NMSP and Location information for a switch using the System left sidebar menu.

To view the NMSP and Location information for a switch, choose **Monitor > Switches**, then click an IP address in the IP Address column. Choose **System > NMSP and Location**.

The NMSP and Location page appears.

You can view the NMSP Status in the NMSP Status group box and Location information in the Location group box.

For more information on NMSP and Location, see the Configuring Switch NMSP and Location.

Monitoring Switch Interfaces

Choose **Monitor > Switches**, then click an IP address in the IP Address column. From the System menu, choose **Interfaces**, then select one of the following interfaces described in this section. This section contains the following topics:

Monitoring Switch Ethernet Interfaces

Choose **Monitor > Switches**, then click an IP address in the IP Address column. From the System menu, choose **Interfaces > Ethernet Interfaces**. Table 5-35 describes the Ethernet interface information that is displayed.

Table 5-35 Viewing Switch Ethernet Interfaces

Name	Name of the Ethernet interface. Click an Ethernet interface name to see details as described in "Monitoring Switch Ethernet Interface Details" section on page 5-41.
MAC Address	MAC address of the Ethernet interface.
Speed (Mbps)	Estimate of the current bandwidth of the Ethernet interface in bits per second.
Operational Status	Current operational state of the Ethernet interface.
MTU	Size of the largest packet that can be sent/received on the interface.
Desired VLAN Mode	VLAN mode.
Access VLAN	VLAN on which the port is configured.

Monitoring Switch Ethernet Interface Details

Choose **Monitor > Switches**, then click an IP address in the IP Address column. From the System menu, choose **Interfaces > Ethernet Interfaces**, then click an Ethernet interface name in the Name column. Table 5-36 describes the Ethernet interface detail information that is displayed.

Table 5-36 Viewing Switch Ethernet Interface Details

Ethernet Interfaces	
Name	Name of the Ethernet interface.
Admin Status	Administration status of the interface.
Duplex Mode	Duplex mode configured on the interface.
VLAN Switch Port	
Operational VLAN Mode	Specifies the operational mode of the VLAN switch port, which can be either an access port or a trunk port.
Desired VLAN Mode	VLAN mode, which can be truck, access, dynamic, or desirable.
Access VLAN	VLAN on which the port is configured.
Operational Truck Encapsulation	Trunk encapsulation, which can be *802.1Q* or *none*.
VLAN Trunk	
Native VLAN	Untagged VLAN on the trunk switch port.
Prune Eligible	Specifies whether VLANs on the trunk port can be pruned.
Allows VLANs	List of allowed VLANs on the trunk port.
Desired Trunking Encapsulation	Trunk encapsulation.
Trunking Encapsulation Negotiation	Specifies that the interface negotiate with the neighboring interface to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring interface.

Monitoring Switch IP Interfaces

Choose **Monitor > Switches**, then click an IP address in the IP Address column. From the System menu, choose **Interfaces > IP Interfaces**. Table 5-37 describes the IP interface information that is displayed.

Table 5-37 Viewing Switch IP Interfaces

Interface	Name of the interface.
IP Address	IP address of the interface.
Address Type	Type of address (IPv4 or IPv6).

Monitoring Switch VLAN Interfaces

Choose **Monitor > Switches**, then click an IP address in the IP Address column. From the System menu, choose **Interfaces > VLAN Interfaces**. Table 5-38 describes the VLAN interface information that is displayed.

Table 5-38 Viewing Switch VLAN Interfaces

Port Name	Name of the VLAN port.
VLAN ID	ID of the VLAN port.
Operational Status	Current operational state of the VLAN interface.
Admin Status	Current administrative state of the VLAN interface.
Port Type	Type of VLAN port.
Maximum Speed (Mbps)	Maximum supported speed for the VLAN interface.
MTU	Size of the largest packet that can be sent/received on the VLAN interface.

Monitoring Switch EtherChannel Interfaces

Choose **Monitor > Switches**, then click an IP address in the IP Address column. From the System menu, choose **Interfaces > EtherChannel Interfaces**. Table 5-39 describes the EtherChannel interface information that is displayed.

Table 5-39 Viewing Switch EtherChannel Interfaces

Name	Name of the EtherChannel interface.
Channel Group ID	Numeric identifier for the EtherChannel.
Control Method	Protocol for managing the EtherChannel either LACP or TAgP.
Actor Admin Key	Channel Identifier.
Number of (LAG) Members	Number of ports configured.

Monitoring Switch Clients

Choose **Monitor > Switches**, then click an IP address in the IP Address column. From the System menu, choose **Clients**. Table 5-39 describes the EtherChannel interface information that is displayed.

Table 5-40 Viewing Current Associated Client

IP Address	IP address of the client.
MAC Address	MAC address of the client.

Table 5-40 Viewing Current Associated Client

User Name	Username of the client.
Vendor Name	Vendor Name of the client.
Map Location	Location of the client.
VLAN	VLAN on which the client is configured.
Interface	Interface on which the client is configured.
Association Time	Timestamp of the client association.
Authorization Profile Name	Authorization Profile Name stored.

Monitoring Access Points

This section describes access to the controller access points summary details. Use the main date area to access the respective access point details.

Choose **Monitor > Access Points** to access this page. This section provides more detailed information regarding monitoring access points and contains the following topics:

Searching Access Points

Use the NCS Search feature to find specific access points or to create and save custom searches. See one of the following topics for additional information:

Viewing a List of Access Points

Choose **Monitor > Access Points** or perform an access point search to access this page.

This page enables you to view a summary of access points including the default information listed in Table 5-41.

Table 5-41 Access Point Search Results

Field	Description
AP Name Ethernet MAC	The name assigned to the access point. Click a list item to view access point details. See the "Monitoring Access Points Details" section on page 5-57 for more information.
IP Address	Local IP address of the access point.
Radio	Protocol of the rogue access point is 802.11a, 802.11b or 802.11g. Click a list item to view access point radio details. See the "Monitoring Access Point Radio Details" section on page 5-71 for more information.
Map Location	Click a list item to go to the location indicated on the list.
Controller	Click a list item to display a graphic and information about the controller. See the "Monitoring System Summary" section on page 5-4 for more information.
Client Count	Displays the total number of clients currently associated with the controller.
Admin Status	Displays the administration state of the access point as either enabled or disabled.
AP Mode	Displays the operational mode of the access point.
Oper Status	Displays the operational status of the Cisco WLAN Solution device, either Up or Down. If the admin status is disabled, the operation status is labeled as down and there are no alarms.
Alarm Status	Alarms are color coded as follows: – Clear—No Alarm – Red—Critical Alarm – Orange—Major Alarm – Yellow—Minor Alarm **Note** This status is radio alarm status ONLY and does not includes the admin status in the operation status.

Configuring the Access Point List Display

To add, remove, or reorder columns in the table, click the **Edit View** link to go to the Edit View page. Table 5-42 lists the optional access point parameters available for the search results.

Table 5-42 Edit View Search Results

Field	Description
AP Type	Indicates the type of access point (unified or autonomous).
Antenna Azim. Angle	Indicates the horizontal angle of the antenna.
Antenna Diversity	Indicates if antenna diversity is enabled or disabled. Antenna diversity refers to the access point sampling the radio signal from two integrated antenna ports to choose the preferred antenna.
Antenna Elev. Angle	Indicates the elevation angle of the antenna.
Antenna Gain	The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.
Antenna Mode	Indicates the antenna mode such as omni, directional, or non-applicable.
Antenna Name	Indicates the antenna name or type.
Audit Status	Indicates one of the following audit statuses: – Mismatch—Configuration differences were found between the NCS and controller during the last audit. – Identical—No configuration differences were found during the last audit. – Not Available—Audit status is unavailable.
Base Radio MAC	Indicates the MAC address of the base radio.
Bridge Group Name	Indicates the name of the bridge group used to group the access points, if applicable.
CDP Neighbors	Indicates all directly connected Cisco devices.
Channel Control	Indicates whether the channel control is automatic or custom.
Channel Number	Indicates the channel on which the Cisco Radio is broadcasting.
Controller Port	Indicates the number of controller ports.
Google Earth Location	Indicates whether or not a Google Earth location is assigned and indicates the location.
Location	Indicates the physical location of the access point.

Table 5-42 Edit View Search Results (continued)

Field	Description
Node Hops	Indicates the number of hops between access points.
OfficeExtend AP	Specifies whether or not OfficeExtend access is enabled. If it is disabled, the access point is remotely deployed which increases the security risk.
PoE Status	Indicates the power over Ethernet status of the access point. The possible values include the following: – Low—The access point draws low power from the Ethernet. – Lower than 15.4 volts—The access point draws lower than 15.4 volts from the Ethernet. – Lower than 16.8 volts—The access point draws lower than 16.8 volts from the Ethernet. – Normal—The power is high enough for the operation of the access point. – Not Applicable—The power source is not from the Ethernet.
Primary Controller	Indicates the name of the primary controller for this access point.
Radio MAC	Indicates the radio MAC address.
Reg. Domain Supported	Indicates whether or not the regulatory domain is supported.
Serial Number	Indicates the access point serial number.
Slot	Indicates the slot number.
Tx Power Control	Indicates whether the transmission power control is automatic or custom.
Tx Power Level	Indicates the transmission power level.
Up Time	Indicates how long the access point has been up in days, hours, minutes and seconds.
WLAN Override Names	Indicates the WLAN override profile names.
WLAN Override	Indicates whether WLAN Override is enabled or disabled.

Configuring the List of Access Points Display

The Edit View page allows you to add, remove, or reorder columns in the Access Points table.

To edit the available columns in the alarms table, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Click the **Edit View** link.

Step 3 To add an additional column to the access points table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the table.

Step 4 To remove a column from the access points table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. All items in the left column are not displayed in the table.

Step 5 Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.

Step 6 Click **Reset** to restore the default view.

Step 7 Click **Submit** to confirm the changes.

Note See the "Viewing a List of Access Points" section on page 5-44 for additional access point fields than can be added through Edit View.

Generating a Report for Access Points

Note You cannot customize any report that you create in the Access Points list (Monitor > Access Points).

To generate a report for access points, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Click to select the access point(s) for which you want to run a report.

Step 3 Choose the applicable report from the Select a report drop-down list.

Step 4 Click **Go**.

Table 5-43 lists the available reports.

Table 5-43 Access Point Reports

Report	Description	Reference
Load	Generates a report with load information.	See the "Monitoring Traffic Load" section on page 5-49 for more information.
Dynamic Power Control	Generates a report with Dynamic Power Control information.	See the "Monitoring Dynamic Power Control" section on page 5-50 for more information.
Noise	Generates a report with Noise information.	See the "Monitoring Access Points Noise" section on page 5-51 for more information.

Table 5-43 Access Point Reports (continued)

Report	Description	Reference
Interference	Generates a report with Interference information.	See the "Monitoring Access Points Interference" section on page 5-51 for more information.
Coverage (RSSI)	Generates a report with Coverage (RSSI) information.	See the "Monitoring Access Points Coverage (RSSI)" section on page 5-52 for more information.
Coverage (SNR)	Generates a report with Coverage (SNR) information.	See the "Monitoring Access Points Coverage (SNR)" section on page 5-52 for more information.
Up/Down Statistics	Time in days, hours and minutes since the last reboot. Generates a report with Up Time information.	See the "Monitoring Access Points Up/Down Statistics" section on page 5-52 for more information.
Voice Statistics	Generates a report for selected access points showing radio utilization by voice traffic.	See the "Monitoring the Access Points Voice Statistics" section on page 5-53 for more information.
Voice TSM Table	Generates a report for selected access points and radio, organized by client device showing QoS status, PLR, and latency of its voice traffic stream.	See the "Monitoring the Access Points Voice TSM Table" section on page 5-53 for more information.
Voice TSM Reports	Graphical representation of the TSM table except that metrics from the clients are averaged together on the graphs.	See the "Monitoring the Access Points Voice TSM Reports" section on page 5-55 for more information.
802.11 Counters	Displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retried frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.	See the "Monitoring Access Points 802.11 Counters" section on page 5-55 for more information.
AP Profile Status	Displays access point load, noise, interference, and coverage profile status.	See the "Monitoring Access Points AP Profile Status" section on page 5-56 for more information.
Air Quality vs. Time	Displays the air quality index of the wireless network during the configured time duration.	See the "Monitoring Air Quality" section on page 5-57 for more information.
Traffic Stream Metrics	Useful in determining the current and historical quality of service (QoS) for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.	See the "Monitoring Access Points Traffic Stream Metrics" section on page 5-56 for more information.

Table 5-43 Access Point Reports (continued)

Report	Description	Reference
Tx Power and Channel	Displays the channel plan assignment and transmit power level trends of devices based on the filtering criteria used when the report was generated. It could help identify unexpected behavior or issues with network performance.	See the "Monitoring Access Points Tx Power and Channel" section on page 5-56 for more information.
VoIP Calls Graph	Helps analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. To be able to gather useful data from this report, VoIP snooping must be enabled on the WLAN. This report displays information in a graph.	See the "Monitoring VoIP Calls" section on page 5-57 for more information.
VoIP Calls Table	Provides the same information as the VoIP Calls Graph report but in table form.	See the "Monitoring VoIP Calls" section on page 5-57 for more information.
Voice Statistics	Helps analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network. To be able to gather useful data from this report, make sure call admission control (CAC) is supported on voice clients.	See the "Monitoring Voice Statistics" section on page 5-57 for more information.
Worst Air Quality APs	Provides a high-level, easy-to-understand metric to facilitate an "at a glance" understanding of where interference problems are impacting the network. Air Quality (AQ) is reported at a channel, floor, and system level and it supports AQ alerts, so that you can be automatically notified when AQ falls below a desired threshold.	See the "Monitoring Air Quality" section on page 5-57 for more information.

Monitoring Traffic Load

Traffic Load is the total amount of bandwidth used for transmitting and receiving traffic. This enables WLAN managers to track network growth and plan network growth ahead of client demand.

To access the access point load report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the check box(es) of the applicable access point(s).

Step 3 From the Generate a report for selected APs drop-down list, choose **Load**.

Step 4 Click **Go**. The Load report displays for the selected access points.

Table 5-44 lists the fields displayed on this page.

Table 5-44 Traffic Load

Field	Description
AP Name	Click the access point name to view access point details. See the "Monitoring Access Points Details" section on page 5-57 for more information.
Radio	Protocol of the rogue access point is either 802.11a, 802.11b or 802.11g. Click the radio to view On-Demand Statistics for this access point. See the "Monitoring Access Point Radio Details" section on page 5-71 for more information.
Attached Client Count	Number of clients attached (Actual and Threshold.)
Channel Utilization	802.11a RF utilization threshold between 0 and 100 percent (Actual and Threshold).
Receive Utilization	802.11a or 802.11b/g RF receive utilization threshold between 0 and 100 percent.
Transmit Utilization	802.11a or 802.11b/g RF transmit utilization threshold between 0 and 100 percent.
Status	Status of the client connection.

Monitoring Dynamic Power Control

To access the access point Load report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the check box(es) of the applicable access point(s).

Step 3 From the Generate a report for selected APs drop-down list, choose **Dynamic Power Control**.

Step 4 Click **Go**. The Dynamic Power Control report displays the selected access points.

Table 5-45 lists the dynamic control fields for access points displayed on this page.

Table 5-45 Dynamic Power Control Page Fields

Field	Description
AP Name	This is the name assigned to the access point. Click an access point name in the list to access its fields. See the "Monitoring Access Points Details" section on page 5-57 for more information.
Radio	Protocol of the rogue access point is either 802.11a, or 802.11b/g. Click a Cisco Radio in the list to access its fields. See the "Monitoring Access Point Radio Details" section on page 5-71 for more information.

Table 5-45 Dynamic Power Control Page Fields (continued)

Field	Description
Current Power Level	Displays the operating transmit power level from the transmit power table. Access point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power. **Note** The power levels and available channels are defined by the Country Code Setting, and are regulated on a country by country basis.
Power Assignment Mode	Dynamic transmit power assignment has three modes: – Automatic—The transmit power is periodically updated for all Cisco 1000 Series lightweight access points that permit this operation. – On Demand—Transmit power is updated when the Assign Now button is selected. – Fixed—No dynamic transmit power assignments occur and value are set to their global default. The default is Automatic. – Recommended Power Level.

Monitoring Access Points Noise

To access the access point Noise report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the check box(es) of the applicable access point(s).

Note If multiple access points are selected, they must have the same radio type.

Step 3 From the Generate a report selected APs drop-down list, choose **Noise**.

Step 4 Click **Go**. The Noise report displays the selected access points.

This page displays a bar graph of noise (RSSI in dBm) for each channel.

Monitoring Access Points Interference

To access the access point Interference report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the check box(es) of the applicable access point(s).

Note If multiple access points are selected, they must have the same radio type.

Step 3 From the Generate a report for selected APs drop-down list, choose **Interference**.

Step 4 Click **Go**. The Interference report displays the selected access points.

This page displays a bar graph of interference (RSSI in dBm) for each channel:

- High interference -40 to 0 dBm.
- Marginal interference -100 to -40 dBm.
- Low interference -110 to -100 dBm.

Monitoring Access Points Coverage (RSSI)

To access the access point Coverage (RSSI) report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the check box(es) of the applicable access point(s).

Step 3 From the Generate a report for selected APs drop-down list, choose **Coverage (RSSI)**.

Step 4 Click **Go**. The Coverage (RSSI) report displays the selected access points.

This page displays a bar graph of client distribution by received signal strength showing the number of clients versus RSSI in dBm.

Monitoring Access Points Coverage (SNR)

To access the access point Coverage (SNR) report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the check box(es) of the applicable access point(s).

Step 3 From the Generate a report for selected APs drop-down list, choose **Coverage (SNR)**.

Step 4 Click **Go**. The Coverage (SNR) report displays the selected access points.

This page displays a bar graph of client distribution by signal-to-noise ratio showing the number of clients versus SNR.

Monitoring Access Points Up/Down Statistics

To access the access point Up/Down Statistics report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the check box of the applicable access point.

Step 3 From the Generate a report for selected APs drop-down list, choose **Up/Down Statistics**.

Click **Go**. The Up/Down Statistics report displays the selected access points.

Note Up Time is time in days, hours, and minutes since the last reboot.

This page displays a line graph of access point up time graphed against time.

If you select more than one access point, the following message appears:

Please select only one AP for the Up Time Report.

Monitoring the Access Points Voice Statistics

This generates a report for selected access points showing radio utilization by voice traffic. The report includes the number of current calls.

Note Voice Statistics reports are only applicable for CAC/WMM clients.

To access the access point Voice Statistics report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the check box(es) of the applicable access point(s).

Step 3 From the Generate a report for selected APs drop-down list, choose **Voice Statistics**.

Click **Go**. The Voice Statistics report displays for the selected access points.

The page displays the following access point voice statistics:

- AP Name—Select an item under AP Name. For more information, see the "Monitoring Access Points Details" section on page 5-57.
- Radio—Select an item under Radio. For more information, see the "Monitoring Access Point Radio Details" section on page 5-71.
- Calls in Progress—Number of calls in progress.
- Roaming Calls in Progress—Number of roaming calls in progress.
- Bandwidth in Use—Percentage of bandwidth in use.

Monitoring the Access Points Voice TSM Table

This generates a report for selected access points and radio, organized by client device showing QoS status, PLR, and latency of its voice traffic stream.

To access the access point Voice TSM Table report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the check box of the applicable access point.

Step 3 From the Generate a report for selected APs drop-down list, choose **Voice TSM Table**.

Step 4 Click **Go**. The Voice Traffic Stream Metrics Table report displays the selected access point.

Table 5-46 lists the Voice Traffic Stream Metrics Table page fields.

Table 5-46 Voice Traffic Stream Metrics Table Page Fields

Field	Description
Time	Time that the statistics were gathered from the access point(s).
Client MAC	MAC address of the client. This shows a list of the clients evaluated during the most recent 90 second interval. The client could be a VoIP phone, laptop, PDA and refers to any client attached to the access point collecting measurements.
QoS	QoS values (packet latency, packet jitter, packet loss, roaming time) which can affect the WLAN are monitored. Access points and clients measure the metrics, access points collect the measurements and send them to the controller. The access points update the controller with traffic stream metric information every 90 seconds and 10 minutes of data is stored at one time.
% PLR (Downlink)	Percentage of packets lost on the downlink (access point to client) during the 90 second interval.
% PLR (Uplink)	Percentage of packets lost on the uplink (client to access point) during the 90 second interval.
Avg Queuing Delay (ms) (Downlink)	Average queuing delay in milliseconds for the downlink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
Avg Queuing Delay (ms) (Uplink)	Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
% Packets > 40 ms Queuing Delay	Percentage of queuing delay packets greater than 40 ms.
% Packets > 20 ms Queuing Delay	Percentage of queuing delay packets greater than 20 ms.
Roaming Delay	Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the first packet is received from the new access point after a successful roam.

Monitoring the Access Points Voice TSM Reports

This report provides a graphical representation of the Voice Traffic Stream Metrics Table except that metrics from the clients are averaged together on the graphs.

To access the access point Voice Traffic Stream Metrics Table report, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the check box of the applicable access point.

Step 3 From the Generate a report for selected APs drop-down list, choose **Voice TSM Reports**.

Click **Go**. The Voice Traffic Stream Metrics Table report displays for the selected access point.

This page displays line graphs of the following downlink and uplink metric information, including times and dates (see Table 5-47).

Table 5-47 Voice Traffic Stream Metrics Table Reports Page Fields

Field	Description
Average Queuing Delay (ms)	Average queuing delay in milliseconds. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
% Packet with less than 10 ms delay	Percentage of packets with less than 10 milliseconds delay.
% Packet with more than 10 < 20 ms delay	Percentage of packets with more than 10 milliseconds delay but less than 20 milliseconds delay.
% Packet with more than 20 < 40 ms delay	Percentage of packets with more than 20 milliseconds delay but less than 40 milliseconds delay.
% Packet with more than 40 ms delay	Percentage of packets with more than 40 milliseconds delay.
Packet Loss Ratio	Ratio of lost packets.
Total Packet Count	Number of total packets.
Roaming Count	Number of packets exchanged for roaming negotiations in this 90 seconds metrics page.
Roaming Delay	Roaming delay in milliseconds.

Monitoring Access Points 802.11 Counters

Displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retried frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.

See the "802.11 Counters" section on page 14-150 for more information on 802.11 Counters reports.

Monitoring Access Points AP Profile Status

Displays access point load, noise, interference, and coverage profile status.

See the "AP Profile Status" section on page 14-92 for more information on AP Profile Status reports.

Monitoring Access Points Radio Utilization

See the "Network Utilization" section on page 14-155 for more information on Radio Utilization reports.

Monitoring Access Points Traffic Stream Metrics

Useful in determining the current and historical quality of service (QoS) for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.

See the "Traffic Stream Metrics" section on page 14-157 for more information on Traffic Stream Metrics reports.

Monitoring Access Points Tx Power and Channel

See the "Tx Power and Channel" section on page 14-160 for more information on Tx Power and Channel reports.

The Current Tx Power Level setting controls the maximum conducted transmit power. The maximum available transmit power varies according to the configured channel, individual country regulation, and access point capability. See the *Product Guide* or data sheet at www.cisco.com for each specific model to determine the access point capability.

The Current Tx Power Level setting of 1 represents the maximum conducted power setting for the access point. Each subsequent power level (for example. 2, 3, 4, and so on.) represents approximately a 50% (or 3dBm) reduction in transmit power from the previous power level.

Note The actual power reduction might vary slightly for different models of access points.

Based on the configured antenna gain, the configured channel, and the configured power level, the actual transmit power at the access point can be reduced so that the specific country regulations are not exceeded.

Note Irrespective of whether you choose Global or Custom assignment method, the actual conducted transmit power at the access point is verified such that country specific regulations are not exceeded.

Command Buttons

- Save—Save the current settings.
- Audit—Discover the present status of this access point.

Monitoring VoIP Calls

VoIP calls reports helps analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. To be able to gather useful data from this report, VoIP snooping must be enabled on the WLAN. This report displays information in a graph.

Click **VoIP Calls Graph** from the Report Launch Pad to open the VoIP Calls Graph Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "VoIP Calls Graph" section on page 14-162 for more information.

Monitoring Voice Statistics

Voice Statistics report helps analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network. To be able to gather useful data from this report, make sure Call Admission Control (CAC) is supported on voice clients. See the "Voice Statistics" section on page 14-165 for more information.

Monitoring Air Quality

To facilitate an "at a glance" understanding of where interference problems are impacting the network, the NCS rolls up the detailed information into a high-level, easy-to- understand metric referred to as Air Quality (AQ). AQ is reported at a channel, floor, and system level and it supports AQ alerts, so that you can be automatically notified when AQ falls below a desired threshold. See the "Monitoring CleanAir Air Quality Events" section on page 5-155 for more information.

Monitoring Access Points Details

The Access Points Details page enables you to view access point information for a single AP.

Choose **Monitor > Access Points** and click an item in the AP Name column to access this page. Depending on the type of access point, the following tabs might be displayed. This section provides the detailed information regarding each Access Points Details page tab and contains the following topics:

General Tab

Note The General tab fields differ between lightweight and autonomous access points.

This section contains the following topics:

General—Lightweight Access Points

Table 5-48 lists the General (for Lightweight Access Points) Tab fields.

Table 5-48 General (for Lightweight Access Points) Tab Fields

Field	Description
General	
AP Name	Operator defined name of access point.
AP IP address, Ethernet MAC address, and Base Radio MAC address	IP address, Ethernet MAC address and Radio MAC address.
Country Code	The codes of the supported countries. Up to 20 countries can be supported per controller. **Note** Access points might not operate properly if they are not designed for use in your country of operation. For a complete list of country codes supported per product, see the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcscod.html.
Link Latency Settings	You can configure link latency on the controller to measure the link between an access point and the controller. See the "Configuring Link Latency Settings for Access Points" section on page 8-213 for more information. – Current Link Latency (in msec)—The current round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back. – Minimum Link Latency (in msec)—Because link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back. – Maximum Link Latency (in msec)—Because link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back.
LWAPP/CAPWAP Uptime	Displays how long the LWAPP/CAPWAP connection has been active.
LWAPP?CAPWAP Join Taken Time	Displays how long the LWAPP/CAPWAP connection has been joined.
Admin Status	The administration state of the access point as either enabled or disabled.
AP Mode	

Table 5-48 General (for Lightweight Access Points) Tab Fields (continued)

Field	Description
Local	Default mode. Data clients are serviced while configured channels are scanned for noise and rogues. The access point goes off-channel for 50 ms and listens for rogues. It cycles through each channel for the period specified under the Auto RF configuration. **Note** To configure Local or FlexConnect access points for the Cisco Adaptive wIPS feature, choose Local or FlexConnect and select the **Enhanced wIPS Engine Enabled** check box.
Monitor	Radio receive only mode. The access point scans all configured channels every 12 seconds. Only deauthenticated packets are sent in the air with an access point configured this way. A monitor mode access point can connect as a client to a rogue acceess point. **Note** To configure access points for Cisco Adaptive wIPS feature, select **Monitor**. Select the **Enhanced wIPS Engine Enabled** check box and choose **wIPS** from the Monitor Mode Optimization drop-down list. Before you can enable an access point to be in wIPS mode, you must disable the access point radios. If you do not disable the access point radio, an error message appears. **Note** Once you have enabled the access point for wIPS, reenable the radios.
Rogue Detector	The access point radio is turned off and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points heard over the network. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.
Sniffer	The access point captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. These packets contain information such as timestamp, signal strength, packet size, and so on. This feature can only be enabled if you run AiroPeek, which is a third-party network analyzer software that supports the decoding of data packets.
FlexConnect	Enables FlexConnect for up to six access points. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. **Note** FlexConnect must be selected to configure an OfficeExtend access point. When the AP mode is FlexConnect, FlexConnect configuration options display including the option to enable OfficeExtend AP and to enable Least Latency Controller Join.
Bridge	This is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The bridge and its wired clients are listed as client in the NCS if the AP mode is set to Bridge, and the access point is bridge capable.

Table 5-48 General (for Lightweight Access Points) Tab Fields (continued)

Field	Description
Spectrum Expert	This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.
Enhanced wIPs Engine	Enabled or Disabled, to enable the monitoring of the security attacks using Cisco Adaptive wIPS feature.
Operational Status	Registered or Not Registered, as determined by the controller.
Registered Controller	The controller to which the access point is registered. Click to display the registered controller details. See the "Monitoring System Summary" section on page 5-4 for more information.
Primary Controller	The name of the primary controller for this access point.
Port Number	The SNMP name of the access point primary controller. The access point attempts to associate with this controller first for all network operations and in the event of a hardware reset.
AP Uptime	Displays how long the access point has been active to receive and transmit.
Map Location	Customer-definable location name for the access point. Click to look at the actual location on a map. Choose **Monitor** > **Access Points** > *name* > **Map Location** for more information.
Google Earth Location	Indicates whether a Google Earth location is assigned.
Location	The physical location where the access point is placed (or Unassigned).
Statistics Timer	This counter sets the time in seconds that the access point sends its DOT11 statistics to the controller.
PoE Status	The power over ethernet status of the access point. The possible values include the following: – Low—The access point draws low power from the Ethernet. – Lower than 15.4 volts—The access point draws lower than 15.4 volts from the Ethernet. – Lower than 16.8 volts—The access point draws lower than 16.8 volts from the Ethernet. – Normal—The power is high enough for the operation of the access point. – Not Applicable—The power source is not from the Ethernet.
Rogue Detection	Indicates whether or not Rogue Detection is enabled. **Note** Rogue detection is disabled automatically for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. For more information regarding OfficeExtend access points, see the *Cisco Wireless LAN Controller Configuration Guide*.
OfficeExtend AP	Indicates whether or not the access point is enabled as an OfficeExtend access point. The default is Enabled.

Table 5-48 General (for Lightweight Access Points) Tab Fields (continued)

Field	Description
Encryption	Indicates whether or not encryption is enabled. **Note** Enabling or disabling encryption functionality causes the access point to reboot which then causes a loss of connectivity for clients. **Note** DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security. Encryption is only available if the access point is connected to a 5500 series controller with a Plus license.
Least Latency Join	The access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.
Telnet Access	Indicates whether or not Telnet Access is enabled.
SSH Access	Indicates whether or not SSH is enabled. **Note** An OfficeExtend access point might be connected directly to the WAN which could allow external access if the default password is used by the access point. Because of this, Telnet and SSH access are disabled automatically for OfficeExtend access points.
Versions	
Software Version	The operating system release.version.dot.maintenance number of the code currently running on the controller.
Boot Version	The operating system bootloader version number.
Inventory Information	
AP Type	Type of Access Point
AP Model	Access point model number.
Cisco IOS Version	The Cisco IOS Release details.
AP Certificate Type	Either Self Signed or Manufacture Installed.
FlexConnect Mode Supported	Indicates if FlexConnect mode is supported or not.
wIPS Profile (when applicable)	
Profile Name	Click the user-assigned profile name to view wIPS profile details.
Profile Version	
Unique Device Identifier (UDI)	
Name	Name of the Cisco AP for access points.
Description	Description of the access point.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial Number	Unique product serial number.
Run Ping Test Link	Click to ping the access point. The results are displayed in a pop-up dialog box.

Table 5-48 General (for Lightweight Access Points) Tab Fields (continued)

Field	Description
Alarms Link	Click to display alarms associated with this access point.
Events Link	Click to display events associated with this access point.

General—Autonomous

Note For autonomous clients, the NCS *only* collects client counts. The client counts in the Monitor page and reports have autonomous clients included. Client search, client traffic graphs, or other client reports (such as Unique Clients, Busiest Clients, Client Association) do *not* include clients from autonomous access points.

Table 5-49 lists the General (for Autonomous Access Points) tab fields.

Table 5-49 General (for Autonomous Access Points) Tab Fields

Field	Description
AP Name	Operator defined name of access point.
AP IP address and Ethernet MAC address	IP address, Ethernet MAC address of the access point.
AP UpTime	Indicates how long the access point has been up in number of days, hours, minutes, and seconds.
Map Location	Customer-definable location name for the access point. Click to look at the actual location on a map. See the "Monitoring Maps" section on page 4-8 for more information.
WGB Mode	Indicates whether or not the access point is in work group bridge mode.
SNMP Info	
SysObjectId	System Object ID.
SysDescription	The system device type and current version of firmware.
SysLocation	The physical location of the device, such as a building name or room in which it is installed.
SysContact	The name of the system administrator responsible for the device.
Versions	
Software Version	The operating system release.version.dot.maintenance number of the code currently running on the controller.
CPU Utilization	Displays the maximum, average, and minimum CPU utilization over the specified amount of time.
Memory Utilization	Displays the maximum, average, and minimum memory utilization over the specified amount of time.

Table 5-49 General (for Autonomous Access Points) Tab Fields (continued)

Field	Description
Inventory Information	
AP Type	Autonomous or lightweight.
AP Model	The Access Point model number.
AP Serial Number	Unique serial number for this access point.
FlexConnect Mode Supported	If FlexConnect mode is supported or not.
Unique Device Identifier (UDI)	
Name	Name of Cisco AP for access points.
Description	Description of access point.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial Number	Unique product serial number.

Note Memory and CPU utilization charts are displayed.

Note Click **Alarms** to display the alarms associated with the access point.
Click **Events** to display events associated with the access point.

Interfaces Tab

Table 5-50 lists the Interfaces tab fields.

Table 5-50 Interfaces Tab Fields

Field	Description
Interface	
Admin Status	Indicates whether the Ethernet interface is enabled.
Operational Status	Indicates whether the Ethernet interface is operational.
Rx Unicast Packets	Indicates the number of unicast packets received.
Tx Unicast Packets	Indicates the number of unicast packets sent.
Rx Non-Unicast Packets	Indicates the number of non-unicast packets received.
Tx Non-Unicast Packets	Indicates the number of non-unicast packets sent.
Radio Interface	
Protocol	802.11a/n or 802.11b/g/n.
Admin Status	Indicates whether the access point is enabled or disabled.
CleanAir Capable	Indicates whether the access point is able to use CleanAir.
CleanAir Status	Indicates the status of CleanAir.
Channel Number	Indicates the channel on which the Cisco Radio is broadcasting.

Table 5-50 Interfaces Tab Fields (continued)

Field	Description
Extension Channel	Indicates the secondary channel on which Cisco radio is broadcasting.
Power Level	Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.
Channel Width	Indicates the channel bandwidth for this radio interface. See the "Configuring 802.11a/n RRM Dynamic Channel Allocation" section on page 8-127 for more information on configuring channel bandwidth. Minimum (default) setting is 20 MHz. Maximum setting is the maximum channel width supported by this radio.
Antenna Name	Identifies the type of antenna.

Click an interface name to view its properties (see Table 5-51).

Table 5-51 Interface Properties

Field	Description
AP Name	Name of the Access Point.
Link speed	Indicates the speed of the interface in Mbps.
RX Bytes	Indicates the total number of bytes in the error-free packets received on the interface.
RX Unicast Packets	Indicates the total number of unicast packets received on the interface.
RX Non-Unicast Packets	Indicates the total number of non-unicast or mulitcast packets received on the interface.
Input CRC	Indicates the total number of CRC error in packets received on the interface.
Input Errors	Indicates the sum of all errors in the packets while receiving on the interface.
Input Overrun	Indicates the number of times the receiver hardware was incapable of handing received data to a hardware buffer because the input rate exceeded the receiver capability to handle the data.
Input Resource	Indicates the total number of resource errors in packets received on the interface.
Runts	Indicates the number of packets that are discarded because they are smaller than the medium minimum packet size.
Throttle	Indicates the total number of times the interface advised a sending NIC that it was overwhelmed by packets being sent and to slow the pace of delivery.
Output Collision	Indicates the total number of packet retransmitted due to an Ethernet collision.
Output Resource	Indicates the total number of resource errors in packets transmitted on the interface.

Table 5-51 Interface Properties (continued)

Field	Description
Output Errors	Indicates the sum of all errors that prevented the final transmission of packets out of the interface.
Operational Status	Indicates the operational state of the physical Ethernet interface on the AP.
Duplex	Indicates the duplex mode of an interface.
TX Bytes	Indicates the total number of bytes in the error-free packets transmitted on the interface.
TX Unicast Packets	Indicates the total number of unicast packets transmitted on the interface.
TX Non-Unicast Packets	Indicates the total number of non-unicast or mulitcast packets transmitted on the interface.
Input Aborts	Indicates the total number of packet aborted while receiving on the interface.
Input Frames	Indicates the total number of packet received incorrectly having a CRC error and a non-integer number of octets on the interface.
Input Drops	Indicates the total number of packets dropped while receiving on the interface because the queue was full.
Unknown Protocol	Indicates the total number of packet discarded on the interface due to an unknown protocol.
Giants	Indicates the number of packets that are discarded because they exceed the maximum packet size of the medium.
Interface Resets	Indicates the number of times that an interface has been completely reset.
Output No Buffer	Indicates the total number of packets discarded because there was no buffer space.
Output Underrun	Indicates the number of times the transmitter has been running faster than the router can handle.
Output Total Drops	Indicates the total number of packets dropped while transmitting from the interface because the queue was full.

CDP Neighbors Tab

Table 5-52 lists the CDP Neighbors tab fields.

Note This tab is visible only when the CDP is enabled.

Table 5-52 CDP Neighbors Tab Fields

Field	Description
AP Name	The name assigned to the access point.
AP IP Address	IP address of the access point.

Table 5-52 CDP Neighbors Tab Fields (continued)

Field	Description
Port No	Port number connected or assigned to the access point.
Local Interface	Identifies the local interface.
Neighbor Name	Name of the neighboring Cisco device.
Neighbor Address	Network address of the neighboring Cisco device.
Neighbor Port	Port of the neighboring Cisco device.
Duplex	Indicates Full Duplex or Half Duplex.
Interface Speed	Speed at which the interface operates.

Current Associated Clients Tab

Table 5-53 lists the Current Associated Clients tab fields.

Note This tab is visible only when there are clients associated to the AP (CAPWAP or Autonomous AP).

Table 5-53 Current Associated Clients Tab Fields

Field	Description
Username	Click the username to view the Monitor Client Details page for this client. See the "Monitoring Clients and Users" section on page 9-10 for more information.
IP Address	IP address of the associated client.
Client MAC Address	Click the client MAC address to view the Monitor Client Details page for this client. See the "Monitoring Clients and Users" section on page 9-10 for more information.
Association Time	Date and time of the association.
UpTime	Time duration of the association.
SSID	User-defined SSID name.
SNR (dB)	Signal to Noise Ratio in dB of the associated client.
RSSI	Received Signal Strength Indicator in dBm.
Bytes Tx	This indicates the total amount of data that has passed through the Ethernet interface either way.
Bytes Rx	This indicate the total amount of data that has been received through the Ethernet interface either way
When the access point is not associated with the controller, then the database is used to retrieve the data (rather than the controller itself). If the access point is not associated, the following fields appear.	
User Name	Username of the client.

Table 5-53 Current Associated Clients Tab Fields (continued)

Field	Description
IP Address	Local IP Address
Client MAC Address	Client MAC Address
Association Time	Timestamp of the client association.
Session Length	Time length of the session
SSID	User-defined SSID name.
Protocol	
Avg. Session Throughput	
Traffic (MB) as before	

Note Click the **Edit View** link to add, remove or reorder columns in the Current Associated Clients table. See the "Configuring the List of Access Points Display" section on page 5-46 for adding a new field using the Edit View.

SSID Tab

Table 5-54 lists the SSID tab fields.

Note This tab is visible only when the access point is Autonomous AP and there are SSIDs configured on the AP.

Table 5-54 SSID Tab

Field	Description
SSID	Service Set Identifier being broadcast by the access point radio.
SSID Vlan	SSID on an access point is configured to recognize a specific VLAN ID or name.
SSID Vlan Name	SSID on an access point is configured to recognize a specific VLAN ID or name.
MB SSID Broadcast	SSID broadcast disabled essentially makes your Access Point invisible unless a wireless client already knows the SSID, or is using tools that monitor or 'sniff' traffic from an AP's associated clients.
MB SSID Time Period	Within this specified time period, internal communication within the SSID continues to work.

Clients Over Time Tab

This tab displays the following charts:

- Client Count on AP—Displays the total number of clients currently associated with an access point over time.
- Client Traffic on AP—Displays the traffic generated by the client connected in the AP distribution over time.

Note The information that appears in the above charts is presented in a time-based graph. For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed. See the "Time-Based Graphs" section on page 6-71 for more information.

Monitoring Access Point Radio Details

Choose **Monitor > Access Points** and click an item in the Radio column to access this page.

Choose **Monitor > Maps** and click an item in the Name column, then click an access point icon to access this page.

Choose **Monitor > Access Points** and click an item in the AP Name column, click **802.11a** or **802.11b** on the AP Interfaces tab to access this page. This page enables you to view access point information for a single 802.11a or 802.11b/g Cisco Radio.

The default is to show On Demand Statistics. Use the View drop-down list to choose a different view:

- Choose On Demand Statistics, and click **Go** to display On Demand Statistics. See the "Monitoring On Demand Statistics" section on page 5-72 for more information.
- Choose Operational Parameters, and click **Go** to display Operational Parameters. See the "Monitoring Operational Parameters" section on page 5-76 for more information.
- Choose 802.11 MAC Counters, and click **Go** to display 802.11 MAC Counters. See the "Monitoring 802.11 MAC Counters" section on page 5-79 for more information.
- Choose View Alarms and, click **Go** to display View Alarms. See the "Monitoring View Alarms" section on page 5-80 for more information.
- Choose View Events and, click **Go** to display View Events. See the "Monitor View Events" section on page 5-81 for more information.

Monitoring On Demand Statistics

To view On Demand Statistics for an access point, click the Radio of the applicable access point in the Monitor > Access Points page. The Radio Details page defaults to On Demand Statistics. See the "Monitoring Access Point Radio Details" section on page 5-71 for more information on radio details.

Note You can also select On Demand Statistics from the View drop-down list located on the Radio Details page.

This page enables you to view the following access point 802.11a or 802.11b Cisco Radio statistics for a single access point.

General

- AP Name—Click to view the access point details. See the "Monitoring Access Points Details" section on page 5-57 for more information.
- AP MAC Address
- Radio
- CleanAir Capable—Indicates if the access point is CleanAir Capable.
- AP in SE-Connect Mode—Yes or No. Indicates if the access point is connected in SE-Connect mode.
- CleanAir Enabled—Indicates if CleanAir is enabled on this access point.
- CleanAir Sensor Status—Indicates the operational status of the CleanAir censor (Up or Down).
- Admin Status—Enabled or disabled.
- Operational Status—Displays the operational status of the Cisco Radios (Up or Down).
- Controller—Click to display controller system details. See the "Monitoring System Summary" section on page 5-4 for more information.
- Channel—The channel upon which the Cisco Radio is broadcasting.
- Extension Channel—Indicates the secondary channel on which Cisco radio is broadcasting.
- Channel Width—Indicates the channel bandwidth for this radio interface. See the "Configuring 802.11a/n RRM Dynamic Channel Allocation" section on page 8-127 for more information on configuring channel bandwidth.
- Power Level—Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

  The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.
- Port—(1 to 24) Port to which the access point is connected.
- Map Location—Click to display the floor map showing the access point location.

Management Frame Protection

- Protection Capability—All Frames
- Validation Capability—All Frames
- MFP Version Supported—Management Frame Protection version supported and configured.

Profile Information

- Noise Profile—Notification sent when Noise Profile state changes between Success and Failure.
- Interference Profile—Notification sent when Interference Profile state changes between Success and Failure.
- Load Profile—Notification sent when Load Profile state changes between Success and Failure.
- Coverage Profile—Notification sent when Coverage Profile state changes between Success and Failure.

Note Click **Success** or **Failure** to view associated alarms.

Noise by Channel (dBm)

Graph showing channel and noise.

Interference by Channel (dBm%)

Graph showing the percentage of interference per channel.

Note Channel Utilization is a combination of Receive Power (RX) + Transmit Power (TX) + Interference. Interference—Access points report on the percentage of the medium taken up by interfering 802.11 transmissions (this can be from overlapping signals from foreign APs, as well as non-neighbors).

Note The channel list (as configured from the RRM page) is scanned completely using the "channel scan duration" field under monitor intervals. For example, if scanning all 11 channels in 2.4 GHz, and using the default duration (180 seconds), you get: 180/11 = 16.36 seconds approximately between each channel that is being scanned.

Load Statistics

- RX Utilization—802.11a or 802.11b/g RF receive utilization threshold between 0 and 100 percent.
- TX Utilization—802.11a or 802.11b/g RF transmit utilization threshold between 0 and 100 percent.
- Channel Utilization—802.11a RF utilization threshold between 0 and 100 percent (Subcolumns for Actual and Threshold).
- Attached Client Count—The number of clients attached.

General Tab

This section describes the information that appears on the General tab and contains the following topics:

% Client Count by RSSI

Graph with % and Received Signal Strength Indicator.

% Client Count by SNR

Graph with % and Signal-to-Noise Ratio.

Channel Utilization (% Busy)

Graph displaying the channel number on the x-axis and channel utilization on the y-axis.

Noise by Channel(dBm)

Graph displaying the channel on the x-axis and power in dBm on the y-axis.

Rx Neighbors

- Radio MAC Address
- AP Name—Click to view access point details.
- Map—Click to view the map.
- Mobility Group-Leader IP Address
- Neighbor Channel
- Channel Bandwidth
- RSSI (dBm)

Channel Utilization Statistics

- Time
- Picc—Percentage of time consumed by received frames from co-channel APs and clients.
- Pib—Percentage of time consumed by interference on the channel which cannot be correctly demodulated.

Note Picc and Pib values should give a good indication of the percentage of time the access point is busy because of co channel interference.

Client Count Over last 24 Hrs

This graph shows the client count specific to the AP radios (in the last 24 hours).

CleanAir Tab

This section describes the information that appears on the CleanAir tab and contains the following topics:

- "Air Quality" section on page 5-75
- "Interference Power" section on page 5-75
- "Non-WiFi Channel Utilization" section on page 5-75
- "Active Interferers" section on page 5-75
- "View Drop-Down List" section on page 5-75

Air Quality

This graph displays the air quality index of the wireless network. A value of 100 indicates the air quality is best and a value of 1 indicates maximum interference.

Interference Power

This graph displays the interference power of the interfering devices on the channel number.

Non-WiFi Channel Utilization

This graph displays the non-WiFi channel utilization of the wireless network.

Active Interferers

This section displays the details of the active interferers on the wireless network. The following details are available:

- Interferer Name—The name of the interfering device.
- Affected Channels—The channel the interfering device is affecting.
- Detected Time—The time at which the interference was detected.
- Severity—The severity index of the interfering device.
- Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.
- RSSI(dBm)—The Received Signal Strength Indicator of the interfering device.

View Drop-Down List

- Choose **On Demand Statistics**, and click **Go** to display On Demand Statistics for this access point radio. See the "Monitoring On Demand Statistics" section on page 5-72 for more information.
- Choose **Operational Parameters**, and click **Go** to display Operational parameters for this access point radio. See the "Monitoring Operational Parameters" section on page 5-76 for more information.
- Choose **802.11 MAC Counters**, and click **Go** to display 802.11 MAC Counters for this access point radio. See the "Monitoring 802.11 MAC Counters" section on page 5-79 for more information.
- Choose **View Alarms**, and click **Go** to display alarms for this access point radio. See the "Monitoring View Alarms" section on page 5-80 for more information.
- Choose **View Events**, and click **Go** to display events for this access point radio. See the "Monitor View Events" section on page 5-81 for more information.

Monitoring Operational Parameters

To view Operational Parameters for an access point radio, follow these steps:

Step 1 Choose **Monitor > Access Points**, click the radio for the applicable access point.

Step 2 From the **View** drop-down list, choose Operational Parameters.

Step 3 Click **Go**.

This page enables you to view configuration information for a single 802.11a or 802.11b Cisco radio.

General

- AP Name—Click to view the access point details. See the "Monitoring Access Points Details" section on page 5-57 for more information.
- AP MAC Address
- Radio

- Admin Status—Enabled or disabled.
- Operational Status—Displays the operational status of the Cisco Radios (Up or Down).
- Controller—Click to display controller system details. See the "Monitoring System Summary" section on page 5-4 for more information.
- Channel—The channel upon which the Cisco Radio is broadcasting.
- Extension Channel—Indicates the secondary channel on which Cisco radio is broadcasting.
- Channel Width—Indicates the channel bandwidth for this radio interface. See the "Configuring 802.11a/n RRM Dynamic Channel Allocation" section on page 8-127 for more information on configuring channel bandwidth.
- Power Level—Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

  The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.
- Port—(1 to 24) Port to which the access point is connected.
- Map Location—Click to display the floor map showing the access point location.

Station Configuration Parameters

- Configuration Type—Automatic or Custom.
- Number of WLANs—1 (one) is the default.
- Medium Occupancy Limit—Indicates the maximum amount of time, in TU, that a point coordinator might control the usage of the wireless medium without relinquishing control for long enough to allow at least one instance of DCF access to the medium. The default value is 100, and the maximum value is 1000.
- CFP Period—The number of DTIM intervals between the start of CFPs.
- CFP Max. Duration—The maximum duration of the CFP in TU that might be generated by the PCF.
- BSSID—MAC address of the access point.
- Beacon Period—The rate at which the SSID is broadcast by the access point, from 100 to 600 milliseconds.
- DTIM Period—The number of beacon intervals that shall elapse between transmission of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.
- Country String—Identifies the country in which the station is operating. The first two octets of this string are the two character country code.

Physical Channel Parameters

- Current Channel—Current operating frequency channel.
- Configuration—Locally customized or globally controlled.
- Current CCA Mode—CCA method in operation. Valid values:
  - Energy detect only (edonly) = 01.
  - Carrier sense only (csonly) = 02.
  - Carrier sense and energy detect (edandcs)= 04.

  - Carrier sense with timer (cswithtimer)= 08.
  - High rate carrier sense and energy detect (hrcsanded)=16.
- ED/TI Threshold—The Energy Detect and Threshold being used to detect a busy medium (frequency). CCA reports a busy medium upon detecting the RSSI above this threshold.

Physical Antenna Parameters

- Antenna Type—Internal or External.
- Diversity—Enabled via the internal antennas or via either Connector A or Connector B. (Enabled or Disabled).

RF Recommendation Parameters

- Channel—802.11a Low Band, Medium Band, and High Band; 802.11b/g.
- Tx Power Level—Zero (0) if Radio Resource Management (RRM) disabled, 1 - 5 if Radio Resource Management (RRM) is enabled.
- RTS/CTS Threshold—Zero (0) if Radio Resource Management (RRM) disabled, 1 - 5 if Radio Resource Management (RRM) is enabled.
- Fragmentation Threshold—Zero (0) if Radio Resource Management (RRM) is disabled.

MAC Operation Parameters

- Configuration Type—Automatic or Custom.
- RTS Threshold—This attribute indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed.

  An RTS/CTS handshake is performed at the beginning of any frame exchange sequence where the MPDU is a Data or Management type, the MPDU has an individual address in the Address1 field, and the length of the MPDU is greater than this threshold. Setting this attribute to be larger than the maximum MSDU size turns off the RTS/CTS handshake for Data or Management type frames transmitted by this STA. Setting this attribute to zero turns on the RTS/CTS handshake for all frames of Data or Management type transmitted by this STA. The default value of this attribute shall be 2347.
- Short Retry Limit—The maximum number of transmission attempts of a frame, the length of which is less than or equal to dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute is 7.
- Long Retry Limit—The maximum number of transmission attempts of a frame, the length of which is greater than dot11RTSThreshold, that shall be made before a failure condition is indicated. The default value of this attribute shall be 4.
- Fragmentation Threshold—The current maximum size, in octets, of the MPDU that might be delivered to the PHY. An MSDU shall be broken into fragments if its size exceeds the value of this attribute after adding MAC headers and trailers. An MSDU or MMPDU shall be fragmented when the resulting frame has an individual address in the Address1 field, and the length of the frame is larger than this threshold. The default value for this attribute shall be the lesser of 2346 or the aMPDUMaxLength of the attached PHY and shall never exceed the lesser of 2346 or the aMPDUMaxLength of the attached PHY. The value of this attribute shall never be less than 256.
- Max Tx MSDU Lifetime—The elapsed time in TU, after the initial transmission of an MSDU, after which further attempts to transmit the MSDU shall be terminated. The default value of this attribute is 512.

- Max Rx Lifetime—The MaxReceiveLifetime shall be the elapsed time in TU, after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU shall be terminated. The default value is 512.

Tx Power

- # Supported Power Levels—Five or fewer power levels, depending on operator preference.
- Tx Power Level x—Access point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

Note The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.

- Tx Power Configuration—Globally controlled or customized for this access point (Custom or Global).
- Current Tx Power Level—Displays the operating transmit power level from the transmit power table.

Monitoring 802.11 MAC Counters

To view Operational Parameters for an access point radio, follow these steps:

Step 1 Choose **Monitor > Access Points**, click the radio for the applicable access point.

Step 2 From the **View** drop-down list, choose **802.11 MAC Counters**.

Step 3 Click **Go**.

This page enables you to view 802.11 MAC Counter information for a single 802.11a or 802.11b Cisco Radio.

General

- AP Name—Click to view the access point details. See the "Monitoring Access Points Details" section on page 5-57 for more information.
- AP MAC Address
- Radio
- Admin Status—Enabled or disabled.
- Operational Status—Displays the operational status of the Cisco Radios (Up or Down).
- Controller—Click to display controller system details. See the "Monitoring System Summary" section on page 5-4 for more information.
- Channel—The channel upon which the Cisco Radio is broadcasting.
- Extension Channel—Indicates the secondary channel on which Cisco radio is broadcasting.

- Channel Width—Indicates the channel bandwidth for this radio interface. See the "Configuring 802.11a/n RRM Dynamic Channel Allocation" section on page 8-127 for more information on configuring channel bandwidth.

Note Minimum (default) setting is 20 MHz. Maximum setting is the maximum channel width supported by this radio.

- Power Level—Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

  The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.
- Port—(1 to 24) Port to which the access point is connected.
- Map Location—Click to display the floor map showing the access point location.

RF Counters

- Tx Fragment Count—This counter is incremented for each successfully received MPDU Data or Management type.
- Multicast Tx Frame Count—This counter increments only when the multicast bit is set in the destination MAC address of a successfully transmitted MSDU. When operating as a STA in an ESS, where these frames are directed to the access point, this implies having received an acknowledgment to all associated MPDUs.
- Tx Failed Count—This counter increments when an MSDU is successfully transmitted after one or more retransmissions.
- Retry Count—This counter increments when an MSDU is successfully transmitted after one or more retransmissions.
- Multiple Retry Count—This counter increments when an MSDU is successfully transmitted after more than one retransmission.
- Frame Duplicate Count—This counter increments when a frame is received that the Sequence Control field indicates is a duplicate.
- RTS Success Count—This counter increments when a CTS is received in response to an RTS.
- RTS Failure Count—This counter increments when a CTS is not received in response to an RTS.
- ACK Failure Count—This counter increments when an ACK is not received when expected.
- Rx Fragment Count—The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
- Multicast Rx Framed Count—This counter increments when a MSDU is received with the multicast bit set in the destination MAC address.
- FCS Error Count—This counter increments when an FCS error is detected in a received MPDU.
- Tx Frame Count—This counter increments for each successfully transmitted MSDU.
- WEP Undecryptable Count—This counter increments when a frame is received with the WEP subfield of the Frame Control field set to one and the WEP On value for the key mapped to the AT MAC address indicates that the frame should not have been encrypted or that frame is discarded due to the receiving STA not implementing the privacy option.

Monitoring View Alarms

To access the View Alarms page from the Monitor Access Points page, follow these steps:

Note When the AP is disassociated, in the Monitor > Access Points page, the radio status has a critical status. There is only one alarm, AP disassociated. This is because radio alarms are correlated to AP disassociated alarm.

Note When the controller goes down, the controller inventory dashlet shows the controller status as critical. But the radio inventory dashlet retains the last known status. In the Monitor > Access Point page, the AP alarm status is shown as "Unknown".

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the Radio Type in the Radio Type column of the applicable access point.

Step 3 From the View drop-down list, choose **View Alarms**.

Step 4 Click **Go**.

For more information on Viewing Alarms, see the "Monitoring Alarms" section on page 5-131.

Monitor View Events

To access the View Events page from the Monitor Access Points page, follow these steps:

Step 1 Choose **Monitor > Access Points**.

Step 2 Select the Radio Type in the Radio Type column of the applicable access point.

Step 3 From the View drop-down list, select **View Events**.

Step 4 Click **Go**.

For more information on viewing events, see the "Monitoring Events" section on page 5-149.

Monitoring Mesh Access Points

Mesh Health monitors the overall health of Cisco Aironet 1500 and 1520 series outdoor access points as well as Cisco Aironet 1130 and 1240 series indoor access points when configured as mesh access points, except as noted. Tracking this environmental information is particularly critical for access points that are deployed outdoors. The following factors are monitored:

- Temperature: Displays the internal temperature of the access point in Fahrenheit and Celsius (Cisco Aironet 1510 and 1520 outdoor access points only).
- Heater status: Displays the heater as on or off (Cisco Aironet 1510 and 1520 outdoor access points only)
- AP Up time: Displays how long the access point has been active to receive and transmit.

- LWAPP Join Taken Time: Displays how long it took to establish the LWAPP connection (excluding Cisco Aironet 1505 access points).
- LWAPP Up Time: Displays how long the LWAPP connection has been active (excluding Cisco Aironet 1505 access points).

Mesh Health information is displayed in the General Properties page for mesh access points.

Note The wIPS mode is not supported in the Cisco Aironet 1500 series mesh access points.

To view the mesh health details for a specific mesh access point, follow these steps:

Step 1 Choose **Monitor > Access Points**. A listing of radios belonging to access points appears.

Note The radio status (not an access point status) is displayed when you choose Monitor > Access Points. The given status is updated frequently from traps and wireless status polling and takes several minutes to reflect actual radio status. The overall status of an access point can be found by viewing the access point on a map.

Note You can also use the New Search button to display the mesh access point summary. With the New Search option, you can further define the criteria of the access points that appear. Search criteria include AP Type, AP Mode, Radio Type, and 802.11n Support.

Step 2 Click the AP Name link to display details for that mesh access point. The General tab for that mesh access point appears.

Note You can also access the General tab for a mesh access point from an NCS map page. To display the page, double-click the mesh access point label. A tabbed page appears and displays the General tab for the selected access point.

To add, remove, or reorder columns in the table, click the **Edit View** link in the Monitor > Access Points page.

Mesh Statistics Tab

Mesh Statistics are reported when a child mesh access point authenticates or associates with a parent mesh access point.

Security entries are removed and no longer displayed when the child mesh access point disassociates from the controller.

The following mesh security statistics are displayed for mesh access points:

- Bridging
- Queue
- Security

To view the mesh statistics for a specific mesh access point, follow these steps:

Step 1 Choose **Monitor > Access Points**. A listing of radios belonging to access points appears.

Note The radio status (not an access point status) is displayed when you choose Monitor > Access Points. The given status is updated frequently from traps and wireless status polling and takes several minutes to reflect actual radio status. The overall status of an access point can be found by viewing the access point on a map.

Note You can also use the New Search button to display the access point summary. With the New Search option, you can further define the criteria of the access points that display. Search criteria includes AP Name, IP address, MAC address, Controller IP or Name, Radio type, and Outdoor area.

Step 2 Click the **AP Name** link of the target mesh access point.

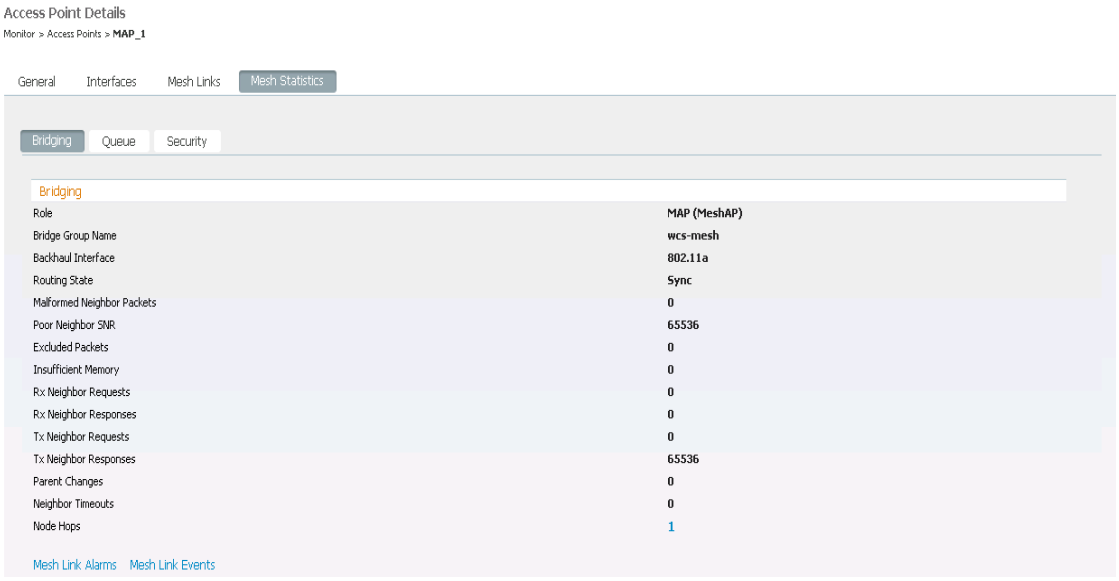
A tabbed page appears and displays the General Properties page for the selected access point.

Step 3 Click the **Mesh Statistics** tab (see Figure 5-1). A three-tabbed Mesh Statistics page appears.

Note The Mesh Statistics tab and its subordinate tabs (Bridging, Queue and Security) only appear for mesh access points. The Mesh Link Alarms and Mesh Link Events links are accessible from each of the three tabbed panels. You can click these links to view the relevant alarms and events.

Note You can also access the Mesh Securities page for a mesh access point from an NCS map. To display the page, double-click the mesh access point label.

Figure 5-1 Monitor > Access Points > AP Name > Mesh Statistics



Summaries of the Bridging, Queue and Security Statistics and their definitions are provided in Table 5-55, Table 5-56 and Table 5-57 respectively.

Table 5-55 Bridging Mesh Statistics

Field	Description
Role	The role of the mesh access point. Options are mesh access point (MAP) and root access point (RAP).
Bridge Group Name	The name of the bridge group to which the MAP or RAP is a member. We recommend assigning membership in a bridge group name. If one is not assigned, a MAP is by default assigned to a default bridge group name.
Backhaul Interface	The radio backhaul for the mesh access point.
Routing State	The state of parent selection. Values that display are seek, scan and maint. Maint appears when parent selection is complete.
Malformed Neighbor Packets	The number of malformed packets received from the neighbor. Examples of malformed packets include malicious floods of traffic such as malformed or short DNS packets and malformed DNS replies.
Poor Neighbor SNR	The number of times the signal-to-noise ratio falls below 12 dB on the backhaul link.
Excluded Packets	The number of packets received from excluded neighbor mesh access points.
Insufficient Memory	The number of insufficient memory conditions.
RX Neighbor Requests	The number of broadcast and unicast requests received from the neighbor mesh access points.
RX Neighbor Responses	The number of responses received from the neighbor mesh access points.
TX Neighbor Requests	The number of unicast and broadcast requests sent to the neighbor mesh access points.
TX Neighbor Responses	The number of responses sent to the neighbor mesh access points.
Parent Changes	The number of times a mesh access point (child) moves to another parent.
Neighbor Timeouts	The number of neighbor timeouts.
Node Hops	The number of hops between the MAP and the RAP. Click the value link to display a dialog box which enables you to configure details of what is reported, how often the node hop value is updated, and view a graphical representation of the report.

Table 5-56 Queue Mesh Statistics

Field	Description
Silver Queue	The average and peak number of packets waiting in the silver (best effort) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Gold Queue	The average and peak number of packets waiting in the gold (video) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Platinum Queue	The average and peak number of packets waiting in the platinum (voice) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Bronze Queue	The average and peak number of packets waiting in the bronze (background) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Management Queue	The average and peak number of packets waiting in the management queue during the defined statistics time interval. Packets dropped and queue size is also summarized.

Table 5-57 Security Mesh Statistics

Field	Description
Packets Transmitted	Summarizes the total number of packets transmitted during security negotiations by the selected mesh access point.
Packets Received	Summarizes the total number of packets received during security negotiations by the selected mesh access point.
Association Request Failures	Summarizes the total number of association request failures that occur between the selected mesh access point and its parent.
Association Request Timeouts	Summarizes the total number of association request time outs that occur between the selected mesh access point and its parent.
Association Request Success	Summaries the total number of successful association requests that occur between the selected mesh access point and its parent.
Authentication Request Failures	Summarizes the total number of failed authentication requests that occur between the selected mesh access point and its parent.

Table 5-57 Security Mesh Statistics (continued)

Field	Description
Authentication Request Timeouts	Summarizes the total number of authentication request timeouts that occur between the selected mesh access point and its parent.
Authentication Request Success	Summarizes the total number of successful authentication requests between the selected mesh access point and its parent mesh node.
Reassociation Request Failures	Summarizes the total number of failed reassociation requests between the selected mesh access point and its parent.
Reassociation Request Timeouts	Summarizes the total number of reassociation request timeouts between the selected mesh access point and its parent.
Reassociation Request Success	Summarizes the total number of successful reassociation requests between the selected mesh access point and its parent.
Reauthentication Request Failures	Summarizes the total number of failed reauthentication requests between the selected mesh access point and its parent.
Reauthentication Request Timeouts	Summarizes the total number of reauthentication request timeouts that occurred between the selected mesh access point and its parent.
Reauthentication Request Success	Summarizes the total number of successful reauthentication requests that occurred between the selected mesh access point and its parent.
Invalid Association Request	Summarizes the total number of invalid association requests received by the parent mesh access point from the selected child mesh access point. This state might occur when the selected child is a valid neighbor but is not in a state that allows association.
Unknown Association Requests	Summarizes the total number of unknown association requests received by the parent mesh access point from its child. The unknown association requests often occur when a child is an unknown neighbor mesh access point.
Invalid Reassociation Request	Summarizes the total number of invalid reassociation requests received by the parent mesh access point from a child. This might happen when a child is a valid neighbor but is not in a proper state for reassociation.

Table 5-57 Security Mesh Statistics (continued)

Field	Description
Unknown Reassociation Request	Summarizes the total number of unknown reassociation requests received by the parent mesh access point from a child. This might happen when a child mesh access point is an unknown neighbor.
Invalid Reauthentication Request	Summarizes the total number of invalid reauthentication requests that occurred between the selected mesh access point and its parent.This state might occur when the selected mesh access point is a valid neighbor but is not in a state that allows reauthentication.

Mesh Links Tab

Table 5-58 lists the Mesh Links tab fields.

Note This tab is visible only for mesh access points. You can click the Mesh Link Alarms and Mesh Link Events links to view the relevant alarms and events.

Table 5-58 Mesh Links Tab Fields

Field	Description
Type	The type of the access point.
AP Name	The name assigned to the access point.
AP MAC Address	The MAC address of the access point.
PER	The Packet Error Rate measured from the total packets that are transmitted in the link test.
Link Detail	Click to view the details of the mesh link alarms, mesh link events, and link metrics.
Link Test	The test used to measure the air link quality between the AP and the neighbor AP.
Channel	The channel number of the mesh access point.
Link SNR (dB)	The air link SNR measured between the AP and the neighbor AP.
SNR Down	The Signal Noise Ratio measured on the air link from the AP to the neighbor AP.
SNR Up	The Signal Noise Ratio measured on the air link from the neighbor AP to the AP.

Note Click the **Edit View** link to add, remove or reorder columns in the Mesh Links table. See the "Configuring the List of Access Points Display" section on page 5-46 for adding a new field using the Edit View.

Retrieving the Unique Device Identifier on Controllers and Access Points

The unique device identifier (UDI) standard uniquely identifies products across all Cisco hardware product families, enabling customers to identify and track Cisco products throughout their business and network operations and to automate their asset management systems. The standard is consistent across all electronic, physical, and standard business communications. The UDI consists of five data elements:

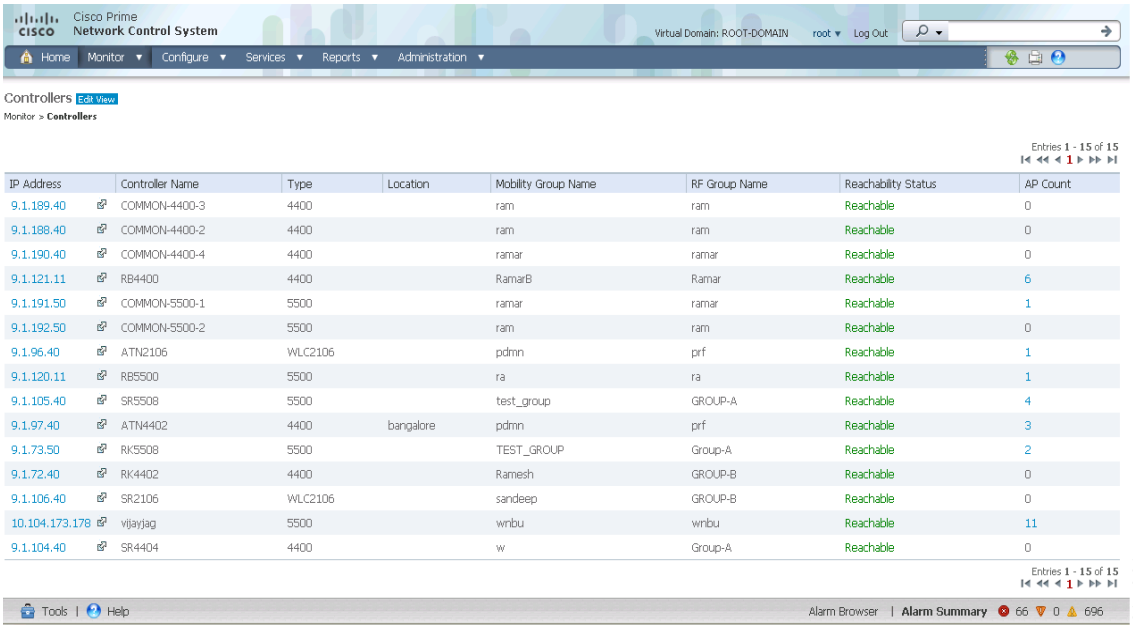
- The orderable product identifier (PID)
- The version of the product identifier (VID)
- The serial number (SN)
- The entity name
- The product description

The UDI is burned into the EEPROM of controllers and lightweight access points at the factory and can be retrieved through the GUI.

To retrieve the UDI on controllers and access points, perform the following steps:

Step 1 Choose **Monitor > Controllers/Access Points**. The Controllers/Access Points page appears (see Figure 5-2).

Figure 5-2 Monitor > Controllers Page



Step 2 Click the IP address of the controller/access point (see in Figure 5-2) whose UDI information you want to retrieve. Data elements of the controller/access point UDI display. These elements are described in Table 5-59..

Table 5-59 Maximum Number of Crypto Cards That can be Installed on a Cisco Wireless LAN Controller

Type of Controller	Maximum Number of Crypto Cards
Cisco 2000 Series	None

Table 5-59 Maximum Number of Crypto Cards That can be Installed on a Cisco Wireless LAN Controller

Type of Controller	Maximum Number of Crypto Cards
Cisco 4100 Series	One
Cisco 4400 Series	Two

Monitoring Coverage Holes

Coverage holes are areas where clients cannot receive a signal from the wireless network. The Cisco Unified Network Solution, radio resource management (RRM) identifies these coverage hole areas and reports them to the NCS, enabling the IT manager to fill holes based on user demand.

The NCS is informed about the reliability-detected coverage holes by the controllers. The NCS alerts the user about these coverage holes. For more information on finding coverage holes, refer to Cisco Context-Aware Services documentation at this location: http://www.cisco.com/en/US/docs/wireless/mse/3350/5.2/CAS/configuration/guide/msecg_ch7_CAS.html

Note Coverage holes are displayed as alarms. Pre-coverage holes are displayed as events.

Monitoring Pre-Coverage Holes

To view pre-coverage hole events, perform these steps:

Step 1 Choose **Monitor > Events** to display all current events.

Step 2 To view pre-coverage hole events only, click the **Advanced Search** link.

Step 3 In the New Search page, change the Search Category drop-down to **Events**.

Step 4 From the Event Category drop-down list, choose **Pre Coverage Hole**, and click **Go**.

The Pre-Coverage Hole Events page provides the information described in Table 5-60.

Table 5-60 Pre-Coverage Hole Fields

Field	Description
Severity	Pre-coverage hole events are always considered informational (Info).
Client MAC Address	MAC address of the client affected by the pre-coverage hole.
AP MAC Address	MAC address of the applicable access point.
AP Name	The name of the applicable access point.
Radio Type	The radio type (802.11b/g or 802.11a) of the applicable access point.
Power Level	Access point transmit power level: 1 = Maximum power allowed per country code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

Table 5-60 Pre-Coverage Hole Fields (continued)

Field	Description
Client Type	Client type can be any of the following: laptop(0) pc(1) pda(2) dot11mobilephone(3) dualmodephone(4) wgb(5) scanner(6) tabletpc(7) printer(8) projector(9) videoconfsystem(10) camera(11) gamingsystem(12) dot11deskphone(13) cashregister(14) radiotag(15) rfidsensor(16) server(17)
WLAN Coverage Hole Status	Determines if the current coverage hole state is enabled or disabled.
WLAN	The name for this WLAN.
Date/Time	The date and time the event occurred. Click the title to toggle between ascending and descending order.

Step 5 Choose a Client MAC Address to view pre-coverage hole details.

- General—Provides the following information:
  - Client MAC Address
  - AP MAC Address
  - AP Name
  - Radio Type
  - Power Level
  - Client Type
  - Category
  - Created
  - Generated By
  - Device AP Address

  - Severity
- Neighbor AP's—Indicates the MAC addresses of nearby access points, their RSSI values, and their radio types.
- Message—Describes what device reported the pre-coverage hole and on which controller it was detected.
- Help—Provides additional information, if available, for handling the event.

Monitoring Rogue Access Points

This section describes security solutions for rogue devices. A rogue device is an unknown access point or client that is detected by managed access points in your network.

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial of service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of clear-to-send (CTS) frames. This action mimics an access point informing a particular client to transmit and instructing all others to wait, which results in legitimate clients being unable to access network resources. Therefore, wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Because rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad-hoc wireless networks without IT department knowledge or consent. These rogue access points can be a serious breach of network security as they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. Even more alarming, wireless users frequently publish insecure access point locations, increasing the odds of having enterprise security breached.

Detecting Rogue Devices

The controllers continuously monitor all nearby access points and automatically discover and collect information on rogue access points and clients. When a controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network.

Note The NCS consolidates all of the controllers rogue access point data.

You can configure controllers to use RLDP on all access points or only on access points configured for monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded RF space, allowing monitoring without creating unnecessary interference and without affecting regular data access point functionality. If you configure a controller to use RLDP on all access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to either manually or automatically contain the detected rogue. See the "Configuring Rogue Policies" section on page 8-108 for information on enabling RLDP.

Note Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, the NCS uses the detecting controller. If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

This section contains the following topics:

Classifying Rogue Access Points

Classification and reporting of rogue access points occurs through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states. You can create rules that enable the controller to organize and display rogue access points as Friendly, Malicious, or Unclassified.

Note The NCS consolidates all of the controllers rogue access point data.

By default, none of the classification rules are enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, and unclassified) in the Alert state only.

Note Rule-based rogue classification does not apply to ad-hoc rogues and rogue clients.

Note The 5500 series controllers support up to 2000 rogues (including acknowledged rogues); the 4400 series controllers, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch support up to 625 rogues; and the 2100 series controllers and Controller Network Module for Integrated Services Routers support up to 125 rogues. Each controller limits the number of rogue containments to three per radio (or six per radio for access points in monitor mode).

When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. The controller verifies that the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.
2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.

3. If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.
4. The controller applies the first rule based on priority. If the rogue access point matches the criteria specified by the rule, the controller classifies the rogue according to the classification type configured for the rule.
5. If the rogue access point does not match any of the configured rules, the controller classifies the rogue as Unclassified.
6. The controller repeats the previous steps for all rogue access points.
7. If RLDP determines that the rogue access point is on the network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can then manually contain the rogue (unless you have configured RLDP to automatically contain the rogue), which would change the rogue state to Contained. If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.
8. If desired, you can manually move the access point to a different classification type and rogue state.

As mentioned previously, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules, or you can manually move the unknown access point to a different classification type and rogue state. Table 5-61 shows the allowable classification types and rogue states from and to which an unknown access point can be configured.

Table 5-61 Allowable Classification Type and Rogue State Transitions

From	To
Friendly (Internal, External, Alert)	Malicious (Alert)
Friendly (Internal, External, Alert)	Unclassified (Alert)
Friendly (Alert)	Friendly (Internal, External)
Malicious (Alert, Threat)	Friendly (Internal, External)
Malicious (Contained, Contained Pending)	Malicious (Alert)
Unclassified (Alert, Threat)	Friendly (Internal, External)
Unclassified (Contained, Contained Pending)	Unclassified (Alert)
Unclassified (Alert)	Malicious (Alert)

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

Rogue access points classification types include:

- Malicious—Detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification. See the "Malicious Rogue APs" section on page 5-94 for more information.
- Friendly—Known, acknowledged, or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained. See the "Friendly Rogue APs" section on page 5-94 for more information. For more information on configuring friendly access point rules, see the "Configuring a Friendly Access Point Template" section on page 10-87.

- Unclassified—Rogue access point that are not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list. See for more information. See the "Unclassified Rogue APs" section on page 5-95 for more information.

Malicious Rogue APs

Malicious rogue access points are detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification.

The Security dashboard of the NCS home page displays the number of malicious rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active malicious rogue access points.

Malicious rogue access point states include:

- Alert—Indicates that the access point is not on the neighbor list or part of the user-configured Friendly AP list.
- Contained—The unknown access point is contained.
- Threat—The unknown access point is found to be on the network and poses a threat to WLAN security.
- Contained Pending—Indicates that the containment action is delayed due to unavailable resources.
- Removed—This unknown access point was seen earlier but is not seen now.

Click an underlined number in any of the time period categories for detailed information regarding the malicious rogue access points. See the "Monitoring Rogue Access Points" section on page 5-91 for more information.

Friendly Rogue APs

Friendly rogue access points are known, acknowledged or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.

Note Only the NCS users can add a rogue access point MAC address to the Friendly AP list. The NCS does not apply the Friendly AP MAC address to controllers.

The Security dashboard of the NCS home page displays the number of friendly rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active friendly rogue access points.

Friendly rogue access point states include the following:

- Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. For example, the access points in your lab network.
- External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. For example, the access points belonging to a neighboring coffee shop.
- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.

Click an underlined number in any of the time period categories for detailed information regarding the friendly rogue access points. See the "Monitoring Rogue Access Points" section on page 5-91 for more information.

To delete a rogue access point from the Friendly AP list, ensure that both the NCS and controller remove the rogue access point from the Friendly AP list. Change the rogue access point from Friendly AP Internal or External to Unclassified or Malicious Alert.

Unclassified Rogue APs

An unclassified rogue access point refers to a rogue access point that is not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list.

The Security dashboard of the NCS home page displays the number of unclassified rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active unclassified rogue access points.

Unclassified rogue access point states include:

- Pending—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point.
- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.
- Contained—The unknown access point is contained.
- Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

Click an underlined number in any of the time period categories for further information. See the "Monitoring Rogue Access Points" section on page 5-91.

Monitoring Rogue AP Alarms

Rogue access point radios are unauthorized access points detected by one or more Cisco 1000 series lightweight access points. To open the Rogue AP Alarms page, do one of the following:

- Search for rogue APs. See the "Using the Search Feature" section on page 2-33 for more information about the search feature.
- From the NCS home page, click the **Security** dashboard. This page displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the **Malicious AP number** link in the Alarm Summary.

Note If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use it to view additional alarms.

Note Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, the NCS uses the detecting controller. If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

The Rogue AP Alarms page contains the following fields:

Note When the NCS polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

- Severity—Indicates the severity of the alarm including the following icons:

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info
	Clear—Appears if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from the NCS after 30 days.

  You can use the Severity Configuration feature to determine the level of severity for the following rogue access point alarm types:

  - Rogue detected
  - Rogue detected contained
  - Rogue detected on network

  See the "Configuring Alarm Severities" section on page 15-71 for more information.

- Rogue MAC Address—Indicates the MAC address of the rogue access points. See the "Viewing Rogue AP Alarm Details" section on page 5-99.
- Vendor—Rogue access point vendor name or Unknown.
- Classification Type—Pending, Malicious, Friendly, or Unclassified.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Strongest AP RSSI—Displays the strongest AP RSSI for this rogue access point across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue access point and your building or location. The higher the RSSI, the closer the location.
- No. of Rogue Clients—Indicates the number of rogue clients associated to this rogue access point.

Note This number comes from the NCS database It is updated every two hours. From the **Monitor > Alarms > Alarm Details** page, this number is a real-time number. It is updated each time you open the Alarm Details page for this rogue access point.

- Owner—Name of person to which this alarm is assigned, or (blank).
- Last Seen Time—Indicates the date and time that the rogue access point was last seen.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point. See the "Classifying Rogue Access Points" section on page 5-92 for additional information.
  - Malicious rogue states include: Alert, Contained, Threat, Contained Pending, and Removed. See the "Malicious Rogue APs" section on page 5-94 for more information.
  - Friendly rogue states include: Internal, External, and Alert. See the "Friendly Rogue APs" section on page 5-94 for more information.
  - Unclassified rogue states include: Pending, Alert, Contained, and Contained Pending. See the "Unclassified Rogue APs" section on page 5-95 for more information.
- SSID—Indicates the service set identifier being broadcast by the rogue access point radio. It is blank if the SSID is not being broadcast.
- Map Location—Indicates the map location for this rogue access point.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user.

  You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the NCS and you can search for all Acknowledged alarms using the alarm search functionality. See the "Acknowledging Alarms" section on page 5-141 for more information.

Note The alarm remains in the NCS, and you can search for all Acknowledged alarms using the alarm search functionality.

Caution When you choose to contain a rogue device, the following warning appears: "There may be legal issues following this containment. Are you sure you want to continue?" The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another network could have legal consequences.

Select a command Menu

Select one or more alarms by selecting their respective check boxes, choose one of the following commands from the Select a command drop-down list, and click **Go**.

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Delete—Delete the selected alarm(s).
- Clear—Clear the selected alarm(s). Indicates that the alarm is no longer detected by any access point.

Note Once the severity is Clear, the alarm is deleted from the NCS after 30 days.

- Acknowledge Alarm—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See the "Acknowledging Alarms" section on page 5-141 for more information.

Note The alarm remains in the NCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge Alarm—Unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the All **Alarms > Email Notification** page to view and configure email notifications. See the "Monitoring RFID Tags" section on page 5-118 for more information.
- Severity Configuration—Allows you to change the severity level for newly-generated alarms. See the "Configuring Alarm Severities" section on page 15-71 for more information.
- Detecting APs—View the Cisco 1000 Series lightweight access points that are currently detecting the rogue access point. See the "Detecting Access Points" section on page 5-112 for more information.
- Map (High Resolution)—Click to display a high-resolution map of the rogue access point location.
- Rogue Clients—Click to view a list of rogue clients associated with this rogue access point. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the Rogue access point. See the "Viewing Rogue Client Details" section on page 5-103 for more information. This information can also be accessed by using the NCS Search feature. See the "Using the Search Feature" section on page 2-33 or the "Advanced Search" section on page 2-34 for more information.
- Set State to 'Unclassified - Alert'—Choose this command to tag the rogue access point as the lowest threat, continue monitoring the rogue access point, and to turn off Containment. See the "Unclassified Rogue APs" section on page 5-95 for more information on Unclassified rogues.
- Set State to 'Malicious - Alert'—Choose this command to tag the rogue access point as 'Malicious'. See the "Malicious Rogue APs" section on page 5-94 for more information on Malicious rogues.
- Set State to 'Friendly - Internal'—Choose this command to tag the rogue access point as internal, add it to the Known Rogue APs list, and to turn off Containment. See the "Friendly Rogue APs" section on page 5-94 for more information on Friendly rogues.
- Set State to 'Friendly - External'—Choose this command to tag the rogue access point as external, add it to the Known Rogue APs list, and to turn off Containment. See the "Friendly Rogue APs" section on page 5-94 for more information on Friendly rogues.
- 1 AP Containment—Target the rogue access point for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue access point for containment by two Cisco 1000 Series lightweight access points.
- 3 AP Containment—Target the rogue access point for containment by three Cisco 1000 Series lightweight access points.
- 4 AP Containment—Target the rogue access point for containment by four Cisco 1000 Series lightweight access points. (Highest containment level.)

Note The higher the threat of the rogue access point, the higher the containment required.

Caution Attempting to contain a rogue access point might lead to legal consequences. When you select any of the AP Containment commands and click **Go**, a message "Containing a Rogue AP may have legal consequences. Do you want to continue?" appears. Click **OK** if you are sure or click **Cancel** if you do not wish to contain any access points.

Viewing Rogue AP Alarm Details

Rogue access point radios are unauthorized access points detected by Cisco 1000 Series lightweight access points. Alarm event details for each rogue access point are available in the Rogue AP Alarms list page.

To view alarm events for a rogue access point radio, click the rogue MAC address for the applicable alarm from the Monitor > Alarms page for rogue access point alarms.

Note All Alarm Details page fields (except No. of Rogue Clients) are populated through polling and are updated every two hours.
The number of rogue clients is a real-time number and is updated each time you access the Alarm Details page for a rogue access point alarm.

Note When the NCS polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

The Alarm Details page displays the following information:

- General
  - Rogue MAC Address—MAC address of the rogue access points.
  - Vendor—Rogue access point vendor name or Unknown.

    Note When a rogue access point alarm displays for Airlink, the vendor displays as Alpha instead of Airlink.

  - Rogue Type—Indicates the rogue type such as AP.
  - On Network—Indicates how the rogue detection occurred.

    Controller—The controller detected the rogue (Yes or No).

    Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
  - Owner—Indicates the owner or is left blank.
  - Acknowledged—Indicates whether or not the alarm is acknowledged by the user.

    You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the NCS and you can search for all Acknowledged alarms using the alarm search functionality. See the "Acknowledging Alarms" section on page 5-141 for more information.

- Classification Type—Malicious, Friendly, or Unclassified.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—Indicates the channel of the rogue access point.
- Containment Level—Indicates the containment level of the rogue access point or Unassigned (not contained).
- Radio Type—Lists all radio types applicable to this rogue access point.
- Strongest AP RSSI—Displays the strongest AP RSSI for this rogue access point across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue access point and your building or location. The higher the RSSI, the closer the location.
- No. of Rogue Clients—Indicates the number of rogue clients associated to this rogue access point.

Note The number of rogue clients is the only real-time field in the **Monitor > Alarm > Alarm Details** page. It updates each time you open the Alarm Details page for this rogue access point.
All other fields on the Alarm Details page are populated through polling and are updated every two hours.

- First Seen Time—Indicates the date and time when the rogue access point was first detected. This information is populated from the controller.
- Last Seen Time—Indicates the date and time when the rogue access point was last detected. This information is populated from the controller.
- Modified—Indicates when the alarm event was modified.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).

  NMS (Network Management System - NCS)—Generated through polling. The NCS periodically polls the controllers and generates events. The NCS generates events when the traps are disabled or when the traps are lost for those events. In this case, “Generated by” is NMS.

  Trap—Generated by the controller. The NCS process these traps and raises corresponding events for them. In this case, “Generated by” is Controller.
- Severity—The severity of the alarm including the following icons:

Icon	Meaning
	Critical
	Major
	Minor
	Warning

Icon	Meaning
	Info
	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from the NCS after 30 days.

You can use the Severity Configuration feature to determine the level of severity for rogue access points. See the "Configuring Alarm Severities" section on page 15-71 for more information.

- Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear.
- Event Details—Click the **Event History** link to view the event details.
- Rogue AP History—Click the **Rogue AP History** link to view the Rogue Alarm details.
- Switch Port Trace Status—Indicates the switch port trace status. Switch port trace status might include: Traced, but not found, Traced and found, Not traced, Failed. See the "Configuring Switch Port Tracing" section on page 15-77 for more information.

- Switch Port Tracing Details—Provides the most recent switch port tracing details. To view additional trace details, click the **Click here for more details** link. See the "Configuring Switch Port Tracing" section on page 15-77 for more information.
- Rogue Clients—Lists rogue clients for this access point including the client MAC address, the last date and time the client was heard, and the current client status. See the "Viewing Rogue Client Details" section on page 5-103 for more information.

Note The number of rogue clients is the only real-time field in the **Monitor > Alarm > Alarm Details** page. It updates each time you open the Alarm Details page for this rogue access point.
All other fields in the Alarm Details page are populated through polling and are updated every two hours.

- Message—Displays the most recent message regarding this rogue access point. A message is sent for the following: When the rogue access point is first detected, for any trap sent, and for any changed state.
- Annotations—Lists current notes regarding this rogue access point. To add a new note, click **New Annotation**. Type the note and click **Post** to save and display the note or **Cancel** to close the page without saving the note.
- Location Notifications—Displays the number of location notifications logged against the client. Clicking a link displays the notifications.
- Location—Provides location information, if available.

Note The switch port tracing does not update any of the rogue attributes such as severity, state, and so on. As the rogue attributes are not updated by switch port tracing, alarms would not be triggered if a rogue is discovered to be 'on network' using switch port tracing.

Select a command Menu

The Select a command drop-down list located in the Rogue AP Alarm Details page provides the following options. Choose an option from the drop-down list, and click **Go**.

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Delete—Delete the selected alarm(s).
- Clear—Clear the selected alarm(s).
- Acknowledge Alarm—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See the "Acknowledging Alarms" section on page 5-141 for more information.

  Note The alarm remains in the NCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- Trace Switch Port—Click to run a switch port trace for this rogue access point. See the "Configuring Switch Port Tracing" section on page 15-77 for more information.
- Event History—Click to view a list of events for this rogue access point. See the "Monitoring Rogue Alarm Events" section on page 5-113 for more information.
- Refresh from Network—Click to sync up the rogue APs from the network.
- View Detecting AP on Network—View the Cisco 1000 Series lightweight access points that are currently detecting the rogue access point. See the "Detecting Access Points" section on page 5-112 for more information.

  Note Detecting AP Name, Radio, SSID information might be empty as the information is not available on controller. Refresh the page after the rogue AP task is completed to see the AP details.

- View Details by Controller—View the classification type and state of the rogue APs reported by the controller.
- Map (High Resolution)—Click to display a high-resolution map of the rogue access point location.
- Rogue Clients—Click to view a list of rogue clients associated with this rogue access point. The Rogue Clients page displays the Client MAC address, when it was last heard, its current status, its controller, and the Rogue access point. See the "Viewing Rogue Client Details" section on page 5-103 for more information. This information can also be accessed by using the NCS Search feature. See the "Using the Search Feature" section on page 2-33 or the "Advanced Search" section on page 2-34 for more information.
- Set State to 'Unclassified - Alert'—Choose this command to tag the rogue access point as the lowest threat, continue monitoring the rogue access point, and to turn off Containment. See the "Unclassified Rogue APs" section on page 5-95 for more information on Unclassified rogues.

- Set State to 'Malicious - Alert'—Choose this command to tag the rogue access point as 'Malicious'. See the "Malicious Rogue APs" section on page 5-94 for more information on Malicious rogues.
- Set State to 'Friendly - Internal'—Choose this command to tag the rogue access point as internal, add it to the Known Rogue APs list, and to turn off Containment. See the "Friendly Rogue APs" section on page 5-94 for more information on Friendly rogues.
- Set State to 'Friendly - External'—Choose this command to tag the rogue access point as external, add it to the Known Rogue APs list, and to turn off Containment. See the "Friendly Rogue APs" section on page 5-94 for more information on Friendly rogues.
- 1 AP Containment—Target the rogue access point for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue access point for containment by two Cisco 1000 series lightweight access points.
- 3 AP Containment—Target the rogue access point for containment by three Cisco 1000 series lightweight access points.
- 4 AP Containment—Target the rogue access point for containment by four Cisco 1000 series lightweight access points. (Highest containment level.)

Note The higher the threat of the rogue access point, the higher the containment required.

Viewing Rogue Client Details

You can view a list of rogue clients in several ways:

- Perform a search for rogue clients using the NCS Search feature. See the "Using the Search Feature" section on page 2-33 for more information.
- View the list of rogue clients for a specific rogue access point from the Alarm Details page for the applicable rogue access point. Click the Rogue MAC address for the applicable rogue client to view the Rogue Client details page.
- In the Alarms Details page of a rogue access point, choose **Rogue Clients** from the Select a command drop-down list.

The Rogue Clients page displays the Client MAC address, when it was last heard, its current status, its controller, and the associated rogue access point.

Note Rogue client statuses include: Contained (the controller contains the offending device so that its signals no longer interfere with authorized clients); Alert (the controller forwards an immediate alert to the system administrator for further action); and Threat (the rogue is a known threat).

Click the Client MAC Address for the rogue client to view the Rogue Client details page. The Rogue Client details page displays the following information:

- General—Information includes: client MAC address, number of access points that detected this client, when the client was first and last heard, the rogue access point MAC address, and the client current status.
- Location Notifications—Indicates the number of notifications for this rogue client including: absence, containment, distance, and all. Click the notification number to open the applicable Monitor > Alarms page.

- APs that detected the rogue client—Provides the following information for all access points that detected this rogue client: base radio MAC address, access point name, channel number, radio type, RSSI, SNR, and the date/time that the rogue client was last heard.
- Location—Provides location information, if available.

Note The higher the threat of the rogue access point, the higher the containment required.

Select a command

The Select a command drop-down list in the Rogue Client details page includes the following options:

- Set State to 'Unknown - Alert'—Choose this command to tag the rogue client as the lowest threat, continue monitoring the rogue client, and to turn off Containment.
- 1 AP Containment—Target the rogue client for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue client for containment by two access points.
- 3 AP Containment—Target the rogue client for containment by three access points.
- 4 AP Containment—Target the rogue client for containment by four access points. (Highest containment level.)
- Map (High Resolution)—Click to display a high-resolution map of the rogue client location.
- Location History—Click to display the history of the rogue client location based on RF fingerprinting.

Viewing Rogue AP History Details

To view the history of a rogue AP alarms, click the **Rogue AP History** link in the Rogue AP Alarm page.

The Rogue AP History page displays the following information:

- Severity—The severity of the alarm.
- Rogue MAC Address—MAC address of the rogue access points.
- Classification Type—Malicious, Friendly, or Unclassified.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Strongest AP RSSI—Displays the strongest AP RSSI for this rogue access point across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue access point and your building or location. The higher the RSSI, the closer the location.
- No. of Rogue Clients—Indicates the number of rogue clients associated to this rogue access point.

Note The number of rogue clients is the only real-time field in the Monitor > Alarm > Alarm Details page. It updates each time you open the Alarm Details page for this rogue access point. All other fields on the Alarm Details page are populated through polling and are updated every two hours.

- First Seen Time—Indicates the date and time when the rogue access point was first detected. This information is populated from the controller.

- Last Seen Time—Indicates the date and time when the rogue access point was last detected. This information is populated from the controller.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Category—Indicates the category of this alarm such as Security or NCS.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Channel Number—Indicates the channel of the ad hoc rogue.
- Containment Level—Indicates the containment level of the ad hoc rogue or Unassigned.
- Switch Port Trace Status—Indicates the switch port trace status. Switch port trace status might include: Traced, but not found, Traced and found, Not traced, Failed.

Click the Rogue MAC address to view the specific rogue AP history details page. The rogue AP history details page displays the above details and also displays the actual alarm message.

Viewing Rogue AP Event History Details

To view the event details of a rogue AP, click the **Event History** link in the Rogue AP Alarm page.

The Rogue AP Event History page displays the following information:

- Severity—The severity of the alarm.
- Rogue MAC Address—MAC address of the rogue access points.
- Vendor—Rogue access point vendor name or Unknown.
- Classification Type—Malicious, Friendly, or Unclassified.
- On Network—Indicates whether the rogue detection occurred.The controller detected the rogue (Yes or No).
- Date/Time—The date and time that the event was generated.
- Radio Type—Lists all radio types applicable to this rogue access point.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Monitoring Ad hoc Rogues

If the MAC address of a mobile client operating in a ad hoc network is not in the authorized MAC address list, then it is identified as an ad hoc rogue. This section contains the following topics:

- Monitoring Ad hoc Rogue Alarms, page 5-106
- Viewing Ad hoc Rogue Alarm Details, page 5-108

Monitoring Ad hoc Rogue Alarms

The Adhoc Rogue Alarms page displays alarm events for ad hoc rogues.To access the Adhoc Rogue Alarms page, do one of the following:

- Perform a search for ad hoc rogue alarms. See the "Using the Search Feature" section on page 2-33 for more information.
- From the NCS home page, click the **Security** dashboard. This page displays all the ad hoc rogues detected in the past hour and the past 24 hours. Click the ad hoc rogue number to view the ad hoc rogue alarms.

If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

The Adhoc Rogue Alarms page contains the following fields:

Note When the NCS polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

- Severity—Indicates the severity of the alarm including the following icons.

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info
	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from the NCS after 30 days.

You can use the Severity Configuration feature to determine the level of severity for the following ad hoc rogue alarm types:

- Adhoc Rogue auto contained
- Adhoc Rogue detected
- Adhoc Rogue detected on network
- Adhoc Rogue detected on network

See the "Configuring Alarm Severities" section on page 15-71 for more information.

- Rogue MAC Address—Indicates the MAC address of the rogue. See the "Viewing Ad hoc Rogue Alarm Details" section on page 5-108 for more information.
- Vendor—Indicates the ad hoc rogue vendor name, or Unknown.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Strongest AP RSSI—Displays the strongest AP RSSI for this rogue across the life of the rogue. The strongest AP RSSI over the life of the rogue displays to indicate the nearest distance that existed between the rogue and your building or location. The higher the RSSI, the closer the location.

  No. of Rogue Clients—Indicates the number of rogue clients associated to this rogue access point.

  Note The number of rogue clients is the only real-time field in the Monitor > Alarm > Alarm Details page. It updates each time you open the Alarm Details page for this rogue access point.
  All other fields in the Alarm Details page are populated through polling and are updated every two hours.

- Owner—Indicates the owner or is left blank.
- Last Seen Time—Indicates the date and time that the alarm was last viewed.
- State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—The Service Set Identifier that is being broadcast by the rogue ad hoc radio. It is blank if there is no broadcast.
- Map Location—Indicates the map location for this ad hoc rogue.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user.

  You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the NCS and you can search for all Acknowledged alarms using the alarm search functionality. See the "Acknowledging Alarms" section on page 5-141 for more information.

Select a command Menu

Select one or more alarms by selecting their respective check boxes, choose one of the following commands from the Select a command drop-down list, and click **Go**.

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Delete—Delete the selected alarm(s).
- Clear—Clear the selected alarm(s).
- Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See the "Acknowledging Alarms" section on page 5-141 for more information.

  Note The alarm remains in the NCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—Unacknowledge an already acknowledged alarm.

- Email Notification—Takes you to the All Alarms > Email Notification page to view and configure email notifications. See the "Monitoring RFID Tags" section on page 5-118 for more information.
- Detecting APs—View the access points that are currently detecting the rogue ad hoc. See the Detecting Access Points, page 112 for more information.
- Map (High Resolution)—Click to display a high-resolution map of the ad hoc rogue location.
- Rogue Clients—Click to view a list of rogue clients associated with this ad hoc rogue. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the ad hoc rogue.
- Set State to 'Alert'—Choose this command to tag the ad hoc rogue as the lowest threat, continue monitoring the rogue access point, and to turn off Containment.
- Set State to 'Internal'—Choose this command to tag the ad hoc rogue as internal, add it to the Known Rogue APs list, and to turn off Containment.
- Set State to 'External'—Choose this command to tag the ad hoc rogue as external, add it to the Known Rogue APs list, and to turn off Containment.
- 1 AP Containment—Target the ad hoc rogue for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the ad hoc rogue for containment by two access points.
- 3 AP Containment—Target the ad hoc rogue for containment by three access points.
- 4 AP Containment—Target the ad hoc rogue for containment by four access points. (Highest containment level.)

Caution Attempting to contain an ad hoc rogue might lead to legal consequences. When you select any of the AP Containment commands and click **Go**, a message "Containing a Rogue AP may have legal consequences. Do you want to continue?" appears. Click **OK** if you are sure, or click **Cancel** if you do not want to contain any access points.

Viewing Ad hoc Rogue Alarm Details

Alarm event details for each ad hoc rogue are available from the Adhoc Rogue Alarms page.

To view alarm events for an ad hoc rogue radio, click the applicable Rogue MAC address in the Adhoc Rogue Alarms page.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by Cisco 1000 Series lightweight access points.

Note When the NCS polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

- General
  - Rogue MAC Address—Media Access Control address of the ad hoc rogue.
  - Vendor—Ad hoc rogue vendor name or Unknown.
  - On Network—Indicates how the rogue detection occurred.

    Controller—The controller detected the rogue (Yes or No).

Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.

- Owner—Indicates the owner or left blank.
- Acknowledged—Indicates whether or not the alarm is acknowledged by the user.

  You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the NCS and you can search for all Acknowledged alarms using the alarm search functionality. See the "Acknowledging Alarms" section on page 5-141 for more information.
- State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—Service Set Identifier being broadcast by the ad hoc rogue radio. (Blank if SSID is not broadcast.)
- Channel Number—Indicates the channel of the ad hoc rogue.
- Containment Level—Indicates the containment level of the ad hoc rogue or Unassigned.
- Radio Type—Lists all radio types applicable to this ad hoc rogue.
- Strongest AP RSSI—Indicates the strongest received signal strength indicator for this NCS (including all detecting access points for all controllers and across all detection times).
- No. of Rogue Clients—Indicates the number of rogue clients associated to this ad hoc.

Note This number comes from the NCS database. It is updated every two hours. In the Monitor > Alarms > Alarm Details page, this number is a real-time number. It is updated each time you open the Alarm Details page for this rogue access point.

- Created—Indicates when the alarm event was created.
- Modified—Indicates when the alarm event was modified.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).

  NMS (Network Management System - NCS)—Generated through polling. The NCS periodically polls the controllers and generates events. The NCS generates events when the traps are disabled or when the traps are lost for those events. In this case, "Generated by" is NMS.

  Trap—Generated by the controller. The NCS process these traps and raises corresponding events for them. In this case, "Generated by" is Controller.
- Severity—Indicates the severity of the alarm including the following icons.

Icon	Meaning
	Critical
	Major
	Minor
	Warning

Icon	Meaning
	Info
	Clear—Appears if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from the NCS after 30 days.

  - Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear. Color coded.

- Annotations—Enter any new notes in this box and click **Add** to update the alarm.
- Message—Displays descriptive information about the alarm.
- Help—Displays the latest information about the alarm.
- Event History—Click to access the Monitor > Events page. See the "Monitoring Events" section on page 5-149 for more information.
- Annotations—Lists existing notes for this alarm.

Searching Rogue Clients Using Advanced Search

When the access points on your wireless LAN are powered up and associated with controllers, the NCS immediately starts listening for rogue access points. When a controller detects a rogue access point, it immediately notifies the NCS, which creates a rogue access point alarm.

To find rogue access point alarms using Advanced Search, follow these steps:

Step 1 Click **Advanced Search** in the top right-hand corner of the NCS main page.

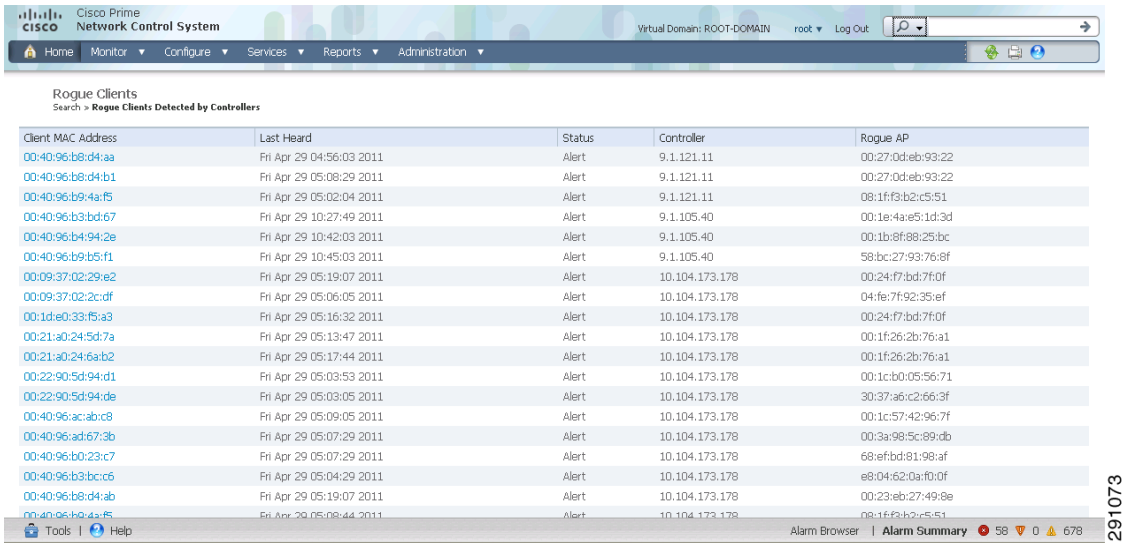
Step 2 Choose **Rogue Client** from the Search Category drop-down list.

Step 3 (Optional) You can filter the search even further with the other search criteria if desired.

Step 4 Click **Search**.

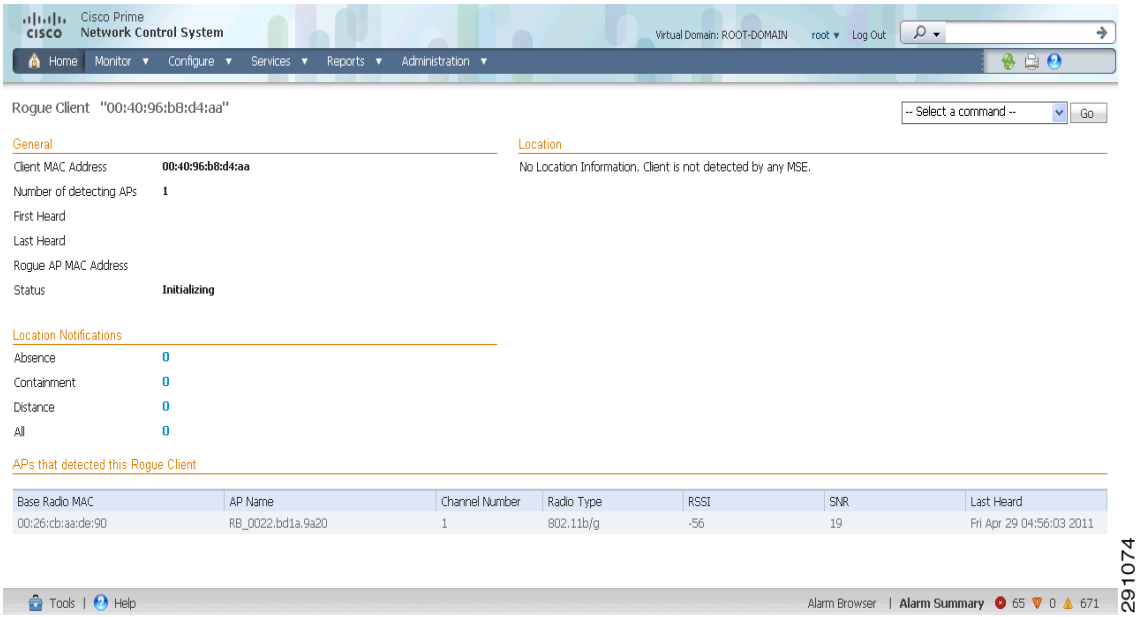
Step 5 The list of rogue clients appears (see Figure 5-3).

Figure 5-3 Rogue Clients Page



Step 6 Choose a rogue client by clicking a client MAC address. The Rogue Client detail page appears (see Figure 5-4).

Figure 5-4 Rogue Client Detail Page



Step 7 To modify the alarm, choose one of these commands from the Select a command drop-down list, and click **Go**.

- Set State to ‘Unknown-Alert’—Tags the ad hoc rogue as the lowest threat, continues to monitor the ad hoc rogue, and turns off containment.
- 1 AP Containment through 4 AP Containment—Indicates the number of access points (1-4) in the vicinity of the rogue unit that send dauthenticate and disassociate messages to the client devices that are associated to the rogue unit.

- Map (High Resolution)—Displays the current calculated rogue location in the Maps > Building Name > Floor Name page.
- Location History—Displays the history of the rogue client location based on RF fingerprinting.

Note The client must be detected by an MSE for the location history to appear.

Monitoring Rogue Access Point Location, Tagging, and Containment

When the Cisco Unified Network Solution is monitored using the NCS, the NCS generates the flags as rogue access point traps and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the access points closest to each rogue access point. The next step is to mark them as Known or Acknowledged rogue access points (no further action), Alert rogue access points (watch for and notify when active), or Contained rogue access points (have between one and four access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

This built-in detection, tagging, monitoring, and containment capability enables system administrators to take appropriate action:

- Locate rogue access points
- Receive new rogue access point notifications, eliminating hallway scans
- Monitor unknown rogue access points until they are eliminated or acknowledged
- Determine the closest authorized access point, making directed scans faster and more effective
- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment can be done for individual rogue access points by MAC address or can be mandated for all rogue access points connected to the enterprise subnet.
- Tag rogue access points:
  - Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or wireless LAN security
  - Accept rogue access points when they do not compromise the LAN or wireless LAN security
  - Tag rogue access points as unknown until they are eliminated or acknowledged
- Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

Detecting Access Points

Use the Detecting Access Points feature to view information about the Cisco lightweight access points that are detecting a rogue access point.

To access the Rogue AP Alarms details page, follow these steps:

Step 1 To display the Rogue AP Alarms page, do one of the following:

- Perform a search for rogue APs. See the "Using the Search Feature" section on page 2-33 for more information about the search feature.
- In the NCS home page, click the **Security** dashboard. This dashboard displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the **Malicious AP** number link in the Alarm Summary box.

Step 2 In the Rogue AP Alarms page, click the Rogue MAC Address for the applicable rogue access point. The Rogue AP Alarms details page appears.

Step 3 From the Select a command drop-down list, choose **Detecting APs**.

Step 4 Click **Go**.

Click a list item to display data about that item:

- AP Name
- Radio
- Map Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio.
- Channel Number—Which channel the rogue access point is broadcasting on.
- WEP—Enabled or disabled.
- WPA—Enabled or disabled.
- Pre-Amble—Long or short.
- RSSI—Received signal strength indicator in dBm.
- SNR—Signal-to-noise ratio.
- Containment Type—Type of containment applied from this access point.
- Containment Channels—Channels that this access point is currently containing.

Monitoring Rogue Alarm Events

The Events page enables you to review information about rogue alarm events. The NCS generates an event when a rogue access point is detected or if you make manual changes to a rogue access point (such as changing its state). The Rogue AP Events list page displays all rogue access point events.

To access the Rogue AP Events list page, follow these steps:

Step 1 Do one of the following:

- Perform a search for rogue access point events using the Advanced Search feature of the NCS. See the "Advanced Search" section on page 2-34 for more information.
- In the Rogue AP Alarms details page, click **Event History** from the Select a command drop-down list. See the "Viewing Rogue AP Alarm Details" section on page 5-99 for more information.

Step 2 The Rogue AP Events list page displays the following event information.

- Severity—Indicates the severity of the alarm including the following icons.

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info

- Rogue MAC Address—Click the rogue MAC address to view the Rogue AP Event Details page. See the "Viewing Rogue AP Event Details" section on page 5-114 for more information.
- Vendor—Rogue access point vendor name or Unknown.
- Classification Type—Malicious, Friendly, or Unclassified.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Date/Time—The date and time that the event was generated.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Viewing Rogue AP Event Details

To view rogue access point event details, follow these steps:

Step 1 In the Rogue AP Events list page, click the **Rogue MAC Address** link.

Step 2 The Rogue AP Events Details page displays the following information:

- Rogue MAC address
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Classification Type—Malicious, Friendly, or Unclassified.

- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- Containment Level—Indicates the containment level of the rogue access point or Unassigned.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Created—The date and time that the event was generated.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  - NMS (Network Management System - NCS)—Generated through polling. The NCS periodically polls the controllers and generates events. The NCS generates events when the traps are disabled or when the traps are lost for those events. In this case, “Generated by” is NMS.
  - Trap—Generated by the controller. The NCS process these traps and raises corresponding events for them. In this case, “Generated by” is Controller.
- Device IP Address
- Severity—Indicates the severity of the alarm including the following icons.

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info
	Clear—Appears if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from the NCS after 30 days.

- Message—Provides details of the current event.

Monitoring Ad hoc Rogue Events

The Events page enables you to review information about ad hoc rogue events. The NCS generates an event when an ad hoc rogue is detected or if you make manual changes to an ad hoc rogue (such as changing its state). The Adhoc Rogue Events list page displays all ad hoc rogue events.

To access the Rogue AP Events list page, follow these steps:

Step 1 Do one of the following:

- Perform a search for ad hoc rogues events using the Advanced Search feature of the NCS. See the "Advanced Search" section on page 2-34 for more information.
- In the Adhoc Rogue Alarms details page, click **Event History** from the Select a command drop-down list. See the "Viewing Ad hoc Rogue Alarm Details" section on page 5-108 for more information.

Step 2 The Rogue AP Events list page displays the following event information.

- Severity—Indicates the severity of the alarm including the following icons.

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info

- Rogue MAC Address—Click the rogue MAC address to view the Rogue AP Event Details page. See the "Viewing Ad hoc Rogue Event Details" section on page 5-117 for more information.
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Date/Time—The date and time that the event was generated.
- State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Viewing Ad hoc Rogue Event Details

To view rogue access point event details, follow these steps:

Step 1 In the Rogue AP Events list page, click the **Rogue MAC Address** link.

Step 2 The Rogue AP Events Details page displays the following information:

- Rogue MAC Address
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- Containment Level—Indicates the containment level of the rogue access point or Unassigned.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Created—The date and time that the event was generated.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  - NMS (Network Management System - NCS)—Generated through polling. The NCS periodically polls the controllers and generates events. The NCS generates events when the traps are disabled or when the traps are lost for those events. In this case, “Generated by” is NMS.
  - Trap—Generated by the controller. The NCS process these traps and raises corresponding events for them. In this case, “Generated by” is Controller.
- Device IP Address
- Severity—Indicates the severity of the alarm including the following icons.

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info
	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from the NCS after 30 days.

- Message—Provides details of the current event.

Monitoring RFID Tags

The Monitor > RFID Tags page allows you to monitor tag status and location on the NCS maps as well as review tag details.

Note This page is only available in the Location version of the NCS.

This section provides information on the tags detected by the location appliance.

Choose **Monitor > RFID Tags** to access this section. By default, the Tag Summary page is displayed.

This section contains the following topics:

Tag Summary

Choose **Monitor > RFID Tags** to access this page.

This page provides information on the number of tags that are detected by MSE. The following fields are displayed in the main data area:

- Device Name—Name of the MSE device.
- Total Tags—Click the number to view tag details. Clicking the number shows the list of tags located by the MSE. Clicking a MAC address shows the tag details pertaining to that MAC address.

Searching Tags

Use the NCS Advanced Search feature to find specific or all tags.

To search for tags in the NCS, follow these steps:

Step 1 Click **Advanced Search**.

Step 2 Choose **Tags** from the Search Category drop-down list.

Step 3 Identify the applicable tag search fields including:

- **Search By**—Choose All Tags, Asset Name, Asset Category, Asset Group, MAC Address, Controller, MSE, Floor Area, or Outdoor Area.

Note Search fields might change depending on the selected category. When applicable, enter the additional field or filter information to help identify the Search By category.

- **Search In**—Choose MSEs or NCS Controllers.
- **Last detected within**—Choose a time increment from 5 minutes to 24 hours. The default is 15 minutes.
- **Tag Vendor**—Select the check box, and choose **Aeroscout**, **G2**, **PanGo**, or **WhereNet**.
- **Telemetry Tags only**—Select the Telemetry Tags only check box to search tags accordingly.

Step 4 Click **Go**.

Viewing RFID Tag Search Results

Use the NCS Advanced Search feature located in the top right of the NCS page to search for tags by asset type (name, category and group), by MAC address, by system (controller or location appliance), and by area (floor area and outdoor area).

Note Search fields might change depending on the selected category. When applicable, enter the additional field or filter information to help identify the Search By category.

You can further refine your search using the Advanced search fields and save the search criteria for future use. Saved search criteria can be retrieved from the Saved Searches located in the navigation bar.

See the "Advanced Search" section on page 2-34 or the "Saved Searches" section on page 2-46 for additional information.

When you click the MAC address of a tag location in a search results page, the following details appear for the tag:

- Tag vendor

  Note This option does not appear when Asset Name, Asset Category, Asset Group or MAC Address are the search criteria for tags.

- Controller to which the tag is associated
- Telemetry data (CCX v1 compliant tags only)
  - Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.

    Note The Telemetry data option only appears when MSE (select for location servers), Floor Area, or Outdoor Area are selected as the Search for tags by option.

    Note Only those vendor tags that support telemetry appear.

- Asset Information (Name, Category, Group)
- Statistics (bytes and packets received)
- Location (Floor, Last Located, MSE, map)

- Location Notification (Absence, Containment, Distance, All)

Note Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.

- Emergency Data (CCX v1 compliant tags only)

Viewing Tag List

Click the **Total Tags number** link to view the Tags List for the applicable device name. The Tag List contains the following information:

- MAC Address
- Asset Name
- Asset Group
- Asset Category
- Vendor Name
- Mobility Services Engine
- Controller
- Battery Status
- Map Location

Monitoring Chokepoints

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be added to the NCS and placed on Floor Maps. They are pushed to the Location Server during synchronization.

Choose **Monitor > Chokepoints**. A page appears displaying a list of found chokepoints. Clicking a link in the Map Location column for a particular chokepoint displays a map that shows the location of the chokepoint.

The following fields are displayed:

- MAC Address—The MAC address of the chokepoint.
- Chokepoint Name—The user-defined name of the chokepoint.
- Entry/Exit Chokepoint—Indicates whether or not the chokepoint is an entry/exit chokepoint.
- Range—The range of the chokepoint in feet.
- Static IP—The static IP address of the chokepoint.
- Map Location—A link to a map showing the location of the chokepoint.

Performing a Chokepoint Search

An advanced search allows you to search for chokepoints.

To perform an advanced search for a chokepoint in the NCS, follow these steps:

Step 1 Click **Advanced Search** located in the top right corner of the NCS.

Step 2 From the New Search page, choose **Chokepoint** from the Search Category drop-down list.

Step 3 Choose the method by which you want to search (by MAC address or chokepoint name) from the Search for Chokepoint by drop-down list.

Step 4 Enter the MAC address or chokepoint name, depending on the search method selected.

Step 5 Click **Search**.

Monitoring Interferers

The Monitor > Interferer page allows you to monitor interference devices detected by the CleanAir enabled access points.

This section provides information on the interferers detected by the CleanAir enabled access points. By default, the Monitoring AP Detected Interferers page is displayed.

This section contains the following topics:

Monitoring AP Detected Interferers

Choose **Monitor > Interferers** to view all the interfering devices detected by the CleanAir enabled access points on your wireless network. This page enables you to view a summary of the interfering devices including the following default information:

- Interferer ID—A unique identifier for the interferer. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, which you can use to find the interfering device. Click this link to know more about the interferer.
- Type—Indicates the category of the interferer. Click to read more about the type of device. A pop-up window appears displaying more details. The categories include the following:
  - Bluetooth link—A Bluetooth link (802.11b/g/n only)
  - Microwave Owen—A microwave oven (802.11b/g/n only)
  - 802.11 FH—An 802.11 frequency-hopping device (802.11b/g/n only)
  - Bluetooth Discovery—A Bluetooth discovery (802.11b/g/n only)
  - TDD Transmitter—A time division duplex (TDD) transmitter
  - Jammer—A jamming device
  - Continuous Transmitter—A continuous transmitter
  - DECT-like Phone—A digital enhanced cordless communication (DECT)-compatible phone

  - Video Camera—A video camera
  - 802.15.4—An 802.15.4 device (802.11b/g/n only)
  - WiFi Inverted—A device using spectrally inverted Wi-Fi signals
  - WiFi Invalid Channel—A device using non-standard Wi-Fi channels
  - SuperAG—An 802.11 SuperAG device
  - Canopy—A Motorola Canopy device
  - Radar—A radar device (802.11a/n only)
  - XBox—A Microsoft Xbox (802.11b/g/n only)
  - WiMAX Mobile—A WiMAX mobile device (802.11a/n only)
  - WiMAX Fixed—A WiMAX fixed device (802.11a/n only)
  - WiFi AOCI—A WiFi device with AOCI
  - Unclassified
- Status—Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir capable access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir capable access point or no longer reacheable by the NCS.
- Severity—Displays the severity ranking of the interfering device.
- Affected Band—Displays the band in which this device is interfering.
- Affected Channels—Displays the affected channels.
- Duty Cycle (%)—The duty cycle of interfering device in percentage.
- Discovered—Displays the time at which it was discovered.
- Last Updated—The last time the interference was detected.
- Floor—The location where the interfering device is present.

Monitoring AP Detected Interferer Details

Choose **Monitor > Interferers >** *Interferer ID* to view this page. This page enables you to view the details of the interfering devices detected by the access points. This page provides the following details about the interfering device.

- Interferer Properties
  - Type—Displays the type of the interfering device detected by the AP.
- Status—The status of the interfering device. Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir capable access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir capable access point or no longer reachable by the NCS.
  - Severity—Displays the severity ranking of the interfering device.
  - Duty Cycle (%)—The duty cycle of interfering device in percentage.
  - Affected Band—Displays the band in which this device is interfering.

  - Affected Channels—Displays the affected channels.
  - Discovered—Displays the time at which it was discovered.
  - Last Updated—The last time the interference was detected.
- Location
  - Floor—The location where this interfering device was detected.
  - Last Located At—The last time where the interfering device was located.
  - On MSE—The mobility server engine on which this interference device was located.
- Clustering Information
  - Clustered By—Displays the IP address of the controller or the MSE that clustered the interferer information from the access point.
  - Detecting APs—Displays the details of the access point that has detected the interfering device. The details include: Access Point Name (Mac), Severity, and Duty Cycle(%).
- Details—Displays a short description about the interfering type.

Select a command

The Select a command drop-down list provides access to the location history of the interfering device detected by the access point. See the "Monitoring AP Detected Interferer Details Location History" section on page 5-123.

Monitoring AP Detected Interferer Details Location History

Choose **Monitor > Interferers >** *Interference Device ID,* then choose **Location History** from the Select a command drop-down list, and click **Go** to view this page.

- Interferer Information—Displays the basic information about the interfering device.
  - Data Collected At—The time stamp at which the data was collected.
  - Type—The type of the interfering device.
  - Severity—The severity index of the interfering device.
  - Duty Cycle—The duty cycle (in percentage) of the interfering device.
  - Affected Channels—A comma separated list of the channels affected.
- Interferer Location History—Displays the location history of the interfering devices.
  - Time Stamp
  - Floor
- Clustering Information
  - Clustered By
- Detecting APs
  - AP Name—The access point that detected the interfering device.
  - Severity—The severity index of the interfering device.
  - Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.
- Location

- Location Calculated At—Displays the time stamp at which this information was generated.
- Floor—Displays location information of the interfering device.
- A graphical view of the location of the interfering device is displayed in a map. Click the Enlarge link to view an enlarged image.

Configuring the Search Results Display

The Edit View page allows you to add, remove, or reorder columns in the AP Detected Interferers Summary page.

To edit the columns in the AP Detected Interferers page, follow these steps:

Step 1 Choose **Monitor > Interferers**. The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir enabled access points.

Step 2 Click the **Edit View** link.

Step 3 To add an additional column to the access points table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the table.

Step 4 To remove a column from the access points table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. All items in the left column are not displayed in the table.

Step 5 Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.

Step 6 Click **Reset** to restore the default view.

Step 7 Click **Submit** to confirm the changes.

Monitoring Spectrum Experts

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to the NCS. This feature allows the NCS to collect and archive and monitor detailed interferer and air quality data from Spectrum Experts in the network.

To access the Monitor Spectrum Experts page, follow these steps:

Step 1 Choose **Monitor > Spectrum Experts**.

Step 2 From the left sidebar menu, you can access the Spectrum Experts Summary page and the Interferers Summary page.

Spectrum Experts Summary

The Spectrum Experts > Summary page is the default page and provides a table of the Spectrum Experts added to the system. The table provides the following Spectrum Expert information:

- Hostname—Displays the hostname or IP Address depending on how it was added. Click the hostname to access the Spectrum Experts Details page.
- Active Interferers—Indicates the current number of interferes being detected by the Spectrum Experts.
- Affected APs—The number of access points seen by the Spectrum Expert that are potentially affected by detected interferers.
- Alarms—The number of active interference traps sent by the Spectrum Expert. Click to access the Alarm page that is filtered to the active alarms for this Spectrum Expert.
- Reachability Status—Indicates “Reachable” in green if the Spectrum Expert is running and sending data to the NCS; otherwise indicates “Unreachable” in red.
- Location—When the Spectrum is a wireless client, a link is available that displays the location of the Spectrum Expert. A red box around the Spectrum Expert indicates the effective range. Click to access the nearest mapped access point.

Interferers Summary

The Interferers > Summary page displays a list of all the Interferers detected over a 30 day interval. The table provides the following Interferers information:

- Interferer ID—An identifier that is unique across different spectrum experts. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, which you can use to find the interfering device.
- Category—Indicates the category of the interferer. Categories include: Bluetooth, Cordless Phones, Microwave Ovens, 802.11 FH, Generic - Fixed-Frequency, Jammers, Generic - Frequency-Hopped, Generic - Continuous.
- Type—Indicates the type of Interferer. Click to access a pop-up description of the type.
- Status—Indicates Active or Inactive.
  - Active—Indicates that the interferer is currently being detected by a spectrum expert.
  - Inactive—Indicates that the interferer is no longer detected by a spectrum expert or the spectrum expert that saw the interferer is no longer reachable by the NCS.
- Discover Time—Indicates the time of discovery.
- Affected Channels—Identifies affected channels.
- Number of APs Affected—An access point is listed as Affected if the following conditions are met:
  - The access point is managed by the NCS.
  - The spectrum expert detects the access point.
  - The spectrum expert detects an interferer on the serving channel of the access point.
- Power—Indicated in dBm.
- Duty Cycle—Indicated in percentage.

  Note 100% indicates the worst value.

- Severity—Indicates the severity ranking of the Interferer.

Note 100% indicates the worst value where 0 indicates no interference.

Interferers Search

Use the NCS Search feature to find specific Interferers or to create and save custom searches. See one of the following topics for additional information:

- Using the Search Feature, page 2-33
- Quick Search, page 2-33
- Advanced Search, page 2-34
- Saved Searches, page 2-46

Spectrum Experts Details

The Spectrum Expert Details page provides all interference details from a single Spectrum Expert. This page updates every 20 seconds providing a real-time look at what is happening on the remote Spectrum Expert and includes the following items:

- Total Interferer Count—As seen by the specific Spectrum Expert.
- Active Interferers Count Chart—Displays a pie chart that groups interferes by category.
- Active Interferer Count Per Channel—Displays the number of interferes grouped by category on different channels.
- AP List—Provides a list of access points detected by the Spectrum Expert that are on channels that have active interferers detected by the Spectrum Expert on those channels.
- Affected Clients List—Provides a list of clients that are currently authenticated/associated to the radio of one of the access points listed in the access point list.

Monitoring WiFi TDOA Receivers

To monitor Wi-Fi TDOA receivers, follow these steps:

Step 1 Choose **Monitor > WiFi TDOA Receivers**. The WiFi TDOA Receiver summary page appears showing all mapped WiFI TDOA receivers.

Step 2 To refine the search criteria when an extensive lists appears, you can search by MAC address or location sensor name.

a. To initiate a search for a TDOA receiver by its MAC address, click the **Advanced Search** link in NCS. Choose **WiFi TDOA Receiver** from the Search Category drop-down list and **MAC Address** from the Search by drop-down list. Enter the MAC address of the TDOA receiver in the available text box, and click **Search**.

b. To initiate a search for a TDOA receiver by its name, click the **Advanced Search** link in the NCS. Choose **WiFi TDOA Receiver** from the Search Category drop-down list and **WiFi TDOA Receivers** from the Search by drop-down list. Enter the name of the TDOA receiver in the available text box, and click **Search**.

If no match exists, then a message indicating that appears in the page. Otherwise the search result displays.

Note See the "Using the Search Feature" section on page 2-33 or the "Advanced Search" section on page 2-34 for more information on the NCS Search feature.

The WiFi TDOA Receivers page displays the following information:

- MAC Address
- WiFi TDOA Receiver Name
- Static IP—Static IP address of the WiFi TDOA receiver.
- Oper Status—Up or down.
- Map Location—Click the Map Location link to view the floor map for this WiFi TDOA receiver. See "Floor Area" for more information on the NCS floor maps.

Note See the "Configuring Wi-Fi TDOA Receivers" section on page 4-61 for more information on adding, configuring, and editing WiFi TDOA receivers.

Monitoring Media Streams

To monitor the media streams configurations, follow these steps:

Step 1 Choose **Monitor > Media Streams**. The Media Streams page appears showing the list of media streams configured across controllers.

The Media Streams page contains a table with the following columns:

- Stream Name—Media Stream name.
- Start IP—Starting IP address of the media stream for which the multicast direct feature is enabled.
- End IP—Ending IP address of the media stream for which the multicast direct feature is enabled.
- State—Operational state of the media stream.
- Max Bandwidth—Indicates the maximum bandwidth that is assigned to the media stream.
- Priority—Indicates the priority bit set in the media stream. The priority can be any number from 1 to 8. A lower value indicates a higher priority. For example, a priority of 1 is highest and a value of 8 is the lowest.
- Violation—Indicates the action to performed in case of a violation. The possible values are as follows:
  - Drop—Indicates that a stream is dropped on periodic revaluation.
  - Best Effort—Indicates that a stream is demoted to best-effort class on periodic reevaluations.
- Policy—Indicates the media stream policy. The possible values are Admit or Deny.
- Controllers—Indicates the number of controllers that use the specified media stream.
- Clients—Indicates the number of clients that use the specified media stream.

Step 2 To view the media stream details, click a media stream name in the Stream column. The Media Streams page appears.

The Media Streams page displays the following group boxes:

- Media Stream Details—Displays the media stream configuration information. This includes the Name, Start Address, End Address, Maximum Bandwidth, Operational Status, Average Packet Size, RRC Updates, Priority, and Violation.
- Statistics—Displays the number of controllers and number of clients that use the selected media stream. Click the controller count to access the list of controllers that use the selected media stream.
- Error—Displays the error, Worst AP, and corresponding floor map for that AP.
- Client Counts—Displays the number of clients for each period.
- Failed Client Counts—Displays the number of clients that failed for each period.

Note The client information is presented in a time-based graph. For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed.

Monitoring Radio Resource Management (RRM)

The operating system security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access points, automatically discover rogue access points.

Radio Resource Management (RRM), built into the Cisco Unified Wireless Network, monitors and dynamically corrects performance issues found in the RF environment.

The NCS would receive traps whenever a change in the transmit power of the access point or channel occurred. These trap events or similar events such as RF regrouping were logged into the NCS events as informational and were maintained by the event dispatcher. The reason behind the transmit power or channel changes (such as signals from neighboring access points, interference, noise, load, and the like) were not evident. You could not view these events and statistics to then perform troubleshooting practices.

Radio Resource Management (RRM) statistics helps to identify trouble spots and provides possible reasons for channel or power level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on grouping the events together (worst performing access points, configuration mismatch between controllers in the same RF group, coverage holes that were detected by access points based on threshold, pre-coverage holes that were detected by controllers, ratios of access points operating at maximum power, and so on).

Note The RRM dashboard information is only available for lightweight access points.

This section contains the following topics:

- Viewing the RRM Dashboard, page 5-130

Channel Change Notifications

Notifications are sent to the NCS RRM dashboard when a channel change occurs. Channel changes depend on the Dynamic Channel Assignment (DCA) configuration where the mode can be set to auto or on demand. When the mode is *auto*, channel assignment is periodically updated for all lightweight access points which permit this operation. When the mode is set to *on demand*, channel assignments are updated based on request. If the DCA is static, no dynamic channel assignments occur, and values are set to their global default.

When a channel change trap is received and a channel change had occurred earlier, the event is marked as Channel Revised; otherwise, the event is marked as Channel Changed. Each event for channel change can be caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur. For example, suppose a channel change is caused by signal, interference, or noise. When the reason code is received in the notification, the reason code is refactored across the reasons. If three reasons caused the event to occur, the reason code is refactored to 1/3 or 0.33 per reason. If ten channel change events are received with the same reason code, all of the three reasons are equally factored to determine the cause of the channel change.

Transmission Power Change Notifications

Notifications are sent to the NCS RRM dashboard when transmission power changes occur. Each event for transmit power changes is caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur.

RF Grouping Notifications

When RRM is run on the controller, dynamic grouping is done, and a new group leader is chosen. Dynamic grouping has three modes: Automatic, Off and Leader. When the grouping is Off, no dynamic grouping occurs, and each switch optimizes only its own lightweight access point parameters. When the grouping is Automatic, switches form groups and elect leaders to perform better dynamic parameter optimization. With grouping automatic, configured intervals (in seconds) represent the period with which the grouping algorithm is run. (Grouping algorithms also run when the group contents change and automatic grouping is enabled.)

Viewing the RRM Dashboard

Choose **Monitor > Radio Resource Management** to access the RRM dashboard.

The dashboard is made up of the following parts:

- The RRM RF Group Summary shows the number of different RF groups.

Note To get the latest number of RF Groups, you have to run the configuration sync background task.

- The RRM Statistics portion shows network-wide statistics
- The Channel Change Reason portion shows why channels changed for all 802.11a/b/g/n radios.

  - Signal—The channel changed because it improved the channel quality for some other neighbor radio(s). Improving the channel quality for some other neighbor radio(s) improved the channel plan of the system as evaluated by the algorithm.
  - Wifi Interference
  - Load
  - Radar
  - Noise
  - Persistent Non-Wifi Interference
  - Major Air Quality Event
  - Other
- The Channel Change shows all events complete with causes and reasons.
- The Configuration Mismatch portion shows comparisons between leaders and members.
- The Coverage Hole portion rates how severe the coverage holes are and gives their location.
- The Percent Time at Maximum Power shows what percent of time the access points were at maximum power and gives the location of those access points.

The following statistics are displayed:

- Total Channel Changes—The sum total of channel changes across 802.11a/b/g/n radios, irrespective of whether the channel was updated or revised. The count is split over a 24-hour and 7-day period. If you click the percentages link or the link under the 24-hour column, a page with details for that access point only appears.
- Total Configuration Mismatches—The total number of configuration mismatches detected over a 24-hour period.
- Total Coverage Hole Events—The total number of coverage hole events over a 24-hour and 7-day period.
- Number of RF Groups—The total number of RF groups (derived from all the controllers which are currently managed by the NCS).
- Configuration Mismatch—The configuration mismatch over a 24-hour period by RF group with details on the group leader.
- APs at MAX Power—The percentage of access points with 802.11a/n radios as a total percentage across all access points which are at maximum power. The maximum power levels are preset and are derived with reference to the preset value.

Note Maximum power is shown in three areas of the RRM dashboard. This maximum power portion shows the current value and is poll driven.

- Channel Change Causes—A graphical bar chart for 802.11a/n radios. The chart is factored based on the reason for channel change. The chart is divided into two parts, each depicting the percentage of weighted reasons causing the event to occur over a 24-hour and 7-day period. Each event for channel change can be caused by multiple reasons, and the weight is equally divided across these reasons. The net reason code is factored and equated to one irrespective of the number of reasons for the event to occur.

- Channel Change - APs with channel changes—Each event for channel change includes the MAC address of the lightweight access point. For each reason code, you are given the most channel changes that occurred for the 802.11a/n access point based on the weighted reason for channel events. This count is split over a 24-hour and 7-day period.
- Coverage Hole - APs reporting coverage holes—The top five access points filtered by IF Type 11 a/n which triggered a coverage hole event (threshold based) are displayed.
- Aggregated Percent Max Power APs—A graphical progressive chart of the total percentage of 802.11a/n lightweight access points which are operating at maximum power to accommodate coverage holes events. The count is split over a 24-hour and 7-day period.

Note This maximum power portion shows the values from the last 24 hours and is poll driven. This occurs every 15 minutes or as configured for radio performance.

- Percent Time at Maximum Power—A list of the top five 802.11a/n lightweight access points which have been operating at maximum power.

Note This maximum power portion shows the value from the last 24 hours and is only event driven.

Monitoring Clients and Users

The Monitor Clients and Users information assists in identifying, diagnosing, and resolving client issues. Using the Monitor Clients and Users feature, you can view a client association history and statistical information. You can also troubleshoot client historical issues. These tools are useful when users complain of network performance as they move throughout a building with their laptop computers. The information might help you assess what areas experience inconsistent coverage and which areas have the potential to drop coverage. See the "Managing Clients" section on page 9-1 for more information.

Monitoring Alarms

This section contains the following topics:

Alarms and Events Overview

An event is an occurrence or detection of some condition in and around the network. For example, it can be a report about radio interference crossing a threshold, the detection of a new rogue access point, or a controller rebooting.

Events are not generated by a controller for each and every occurrence of a pattern match. Some pattern matches must occur a certain number of times per reporting interval before they are considered a potential attack. The threshold of these pattern matches is set in the signature file. Events can then generate alarms which further can generate e-mail notifications if configured as such.

An alarm is a NCS response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), the NCS raises an alarm until the resulting condition no longer occurs. For example, an alarm might be raised while a rogue access point is detected, but the alarm terminates after the rogue has not been detected for several hours.

One or more events can result in a single alarm being raised. The mapping of events to alarms is their correlation function. For example, some IDS events are considered to be network wide so all events of that type (regardless of which access point the event is reported from) map to a single alarm. On the other hand, other IDS events are client-specific. For these, all events of that type for a specific client MAC address map to an alarm which is also specific for that client MAC address, regardless of whether multiple access points report the same IDS violation. If the same kind of IDS violation takes place for a different client, then a different alarm is raised.

An NCS administrator currently has no control over which events generate alarms or when they time out. On the controller, individual types of events can be enabled or disabled (such as management, SNMP, trap controls, and so on).

Viewing List of Alarms

Choose **Monitor > Alarms** to access the Alarm Browser page which provides a list of alarms. You can also hover your mouse cursor over **Alarm Browser** on the toolbar at the bottom of the NCS page to view the Alarm Browser page.

The Alarm Browser lists the following information for each alarm:

- Severity—Severity of the alarm which can be:
  - Critical
  - Major
  - Minor
  - Warning

  - Informational
- Status—Status of the alarm.
- Timestamp—Date and time that the alarm occurred.
- Category—Category assigned to the alarm such as rogue AP, controller, switch, and security.
- Condition—Condition that caused the alarm.
- Owner—Name of the person to whom this alarm is assigned, if one was entered.
- Message—Messages about the alarm.
- Failure Source—Indicates the source of the event (including name and/or MAC address).

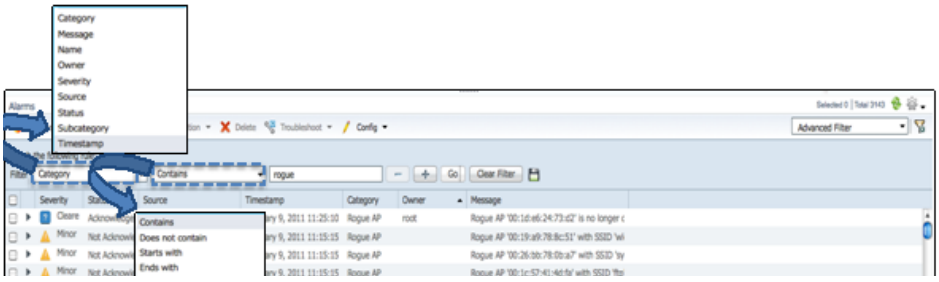
Note By default, acknowledged alarms are not shown in the Alarm Browser page. To change this, choose **Administration > Settings > Alarms**, then unselect the **Hide Acknowledged Alarms** check box. You must unselect the preference of hiding acknowledged alarms if you want acknowledged alarms to show in the NCS Alarm Summary and alarms lists page.

Use the check box to select one or more alarms. To select all alarms displayed in the Alarm Browser, click the topmost box. See the "Modifying Alarms" section on page 5-136 for more information.

Filtering Alarms

In the **Monitor > Alarms** page, you can filter the alarms that are displayed in the Alarm Browser (see Figure 5-5).

Figure 5-5 Filtering Alarms



Choose **Monitor > Alarms**, then from the Show drop-down list, select one of the following filters:

- **Quick Filter**—Enter text in any of the boxes to display alarms that contain the text you enter. For example, if you enter **AP** in the Category field, AP and Rogue AP alarms are displayed. It provides an optional filtered view of alarms for wired and wireless alarms.
- **Advance Filter**—This filter provides an advanced alarm search capability. It provides ability to search on specific fields with various conditions like contains, does not contain, starts with, ends with and so on. Additionally advanced filters allows nesting of AND/OR conditions. Select the category and operator, enter criteria in the text field to compare against, then do the following:
  - Click **+** to add an additional filter or **-** to remove a filter you specified.

- Click **Go** to apply your filter.
- Click **Clear Filter** to clear the entries you entered.
- Click the **disc** icon to save your filter. Enter a name for the filter you want to save, then click **Save**.

Note When you select a preset filter and click the filter button, the filter criteria is dimmed. You can only see the filter criteria but you can not change it. When All is selected to view all the entries, clicking the filter button shows the Quick Filter options, where you can filter the data using the filterable fields. You can also use the free-form box to enter text to filter the table.

- All—Displays all alarms.
- Manage Preset Filter—Displays any previously saved filters and allows you to edit and delete previously saved filters.
- Assigned to Me—Displays all alarms assigned to you.
- Unassigned Alarms—Displays all unassigned alarms.
- Alarms in Last 5 Minutes
- Alarms in Last 15 Minutes
- Alarms in Last 30 Minutes
- Alarms in the last hour
- Alarms in the last 8 hours
- Alarms in the last 24 hours
- Alarms in last 7 days
- All wired alarms—Displays all alarms for wired devices.
- All wireless alarms—Displays all alarms for wireless devices.

Exporting Alarms

You can quickly export the list of alarms into a CSV file (a spreadsheet format with comma-separated values).

Note The columns that are shown in the alarms table are only exported to the CSV file.

To export the list of alarms, follow these steps:

Step 1 Choose **Monitor > Alarms**.

Step 2 Click the icon on the toolbar. A pop-up window appears.

Step 3 In the File Download window, click **Save** to save the file.

Viewing Alarm Details

You can view alarm details in the Monitor > Alarms page by clicking the expand icon to the far left of the Monitor > Alarms page for the alarm for which you want to see details. The details that are displayed depend on the alarm type you selected (see Table 5-62).

Table 5-62 Viewing Alarm Details

Section	Field	Description
General Info[1]	Failure Source	Indicates the source of the event (including name and/or MAC address).
	Owner	Name of person to which this alarm is assigned, or blank.
	Acknowledged	Displays whether or not the alarm is acknowledged by the user.
	Category	The category of the alarm (for example, AP, Rogue AP, or Security).
	Created	Month, day, year, hour, minute, second, AM or PM alarm created.
	Modified	Month, day, year, hour, minute, second, AM or PM alarm last modified.
	Generated By	Device that generated the alarm.
	Severity	Level of security: Critical, Major, Minor, Warning, Clear, Info.
	Previous Severity	The severity of the alarm the after the most recent polling cycle.
Device Info	Device Name	Name of the device.
	Device Address	IP address of the device.
	Device Contact	Contact information for the device.
	Device Location	Location of the device.
	Device Status	Status of the device.
Messages		Device information retrieved from log messages.
Annotation		Lists current notes regarding this rogue access point. To add a new note, click **New Annotation**. Type the note and click **Post** to save and display the note or **Cancel** to close the page without saving the note.

1.The General information might vary depending on the type of alarm. For example, some alarm details might include location and switch port tracing information.

In the Alarms list page, you can also view the events for the alarm you selected as explained in the "Viewing Events Related to Alarms" section on page 5-136.

Viewing Events Related to Alarms

When you select Monitor > Alarms page, you can view alarm summary information by hovering your mouse cursor over an alarm severity in the Severity column and clicking the icon that appears.

A dialog appears displaying the top 5 events related to the alarm you selected.

Click **Events** to display *all* events associated with the selected alarm.

Modifying Alarms

In the Monitor > Alarms page, you can modify the alarms by selecting the check box next to an alarm and then clicking one of the tasks at the top of the Alarm Browser page:

Note The alarms that appear in the Monitor > Alarms page depend on the settings you specify on the Administration > Settings page. See the "Modifying Alarm Settings" section on page 5-139 for more information.

- Change Status—Change the alarm status to one of the following:
  - Acknowledge—You can acknowledge the alarm. By default, acknowledged alarms are not displayed in the Alarm Browser page. Acknowledged alarms remain in the NCS and you can search for all acknowledged alarms using the alarm search functionality. See the "Acknowledging Alarms" section on page 5-141 for more information.
  - Unacknowledge—You can choose to unacknowledge an already acknowledged alarm.
  - Clear—Clear the selected alarm(s). The alarm is removed from the Alarm Browser. Cleared alarms remain in the NCS and you can search for all cleared alarms using the alarm search functionality

  Note Once the severity is Clear, the alarm is deleted from the NCS after 30 days by default. You can modify this setting in the Administration > Settings page.

- Assign—For the selected alarm, you can do the following:
  - Assign to me—Assigns the alarm to the specified user.
  - Unassign—Removes the specified owner from the alarm.
- Annotation—Enter an annotation for the selected alarm, then click **Post**. The annotation you entered appears when you view the alarm details.
- Delete—Delete the selected alarm(s). Indicates that the alarm is no longer detected by any device.

Specifying Email Notifications for Alarms

In the Monitor > Alarms page, you can set up e-mail notifications for alarms based on the alarm category and severity level.

Step 1 Choose **Monitor > Alarms**, then click **Email Notification**.

Step 2 Select the **Enable** check box next to the alarm category for which you want to set up e-mail notifications, then click **Save**.

The NCS sends e-mail notifications when alarms for the categories you specified occur.

Modifying the Alarm Browser

Choose **Monitor > Alarms** to view a list of alarms. You can also click **Alarm Browser** on the toolbar at the bottom of the NCS home page. You can modify the following information displayed in the Alarm Browser:

- To reorder the columns, drag and drop the column headings into any position.
- Click a column heading to sort the information by that column. By default, the column is sorted in descending order. Click the column heading again to change the sort the column in ascending order.

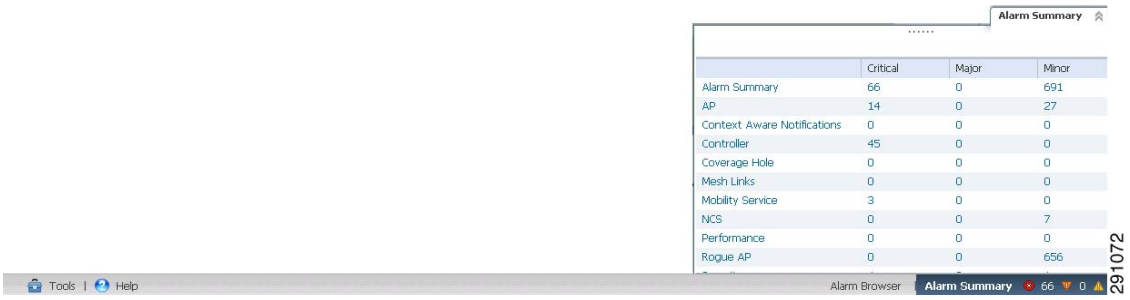
Note Not every column is sortable. Hover your mouse cursor over a column heading, and the NCS displays whether the column is sortable.

- To customize which columns are displayed, click the **Settings** icon, then click **Columns**. Select the check box next to columns you want to appear, and unselect the boxes for the columns you do not want to appear in the Alarm Browser page.

Viewing the Alarm Summary

When the NCS receives an alarm message from a controller, switch, or the NCS, it displays an alarm indicator in the Alarm Summary. The Alarm Summary is at the bottom of the NCS home page and displays the total count of critical, major, and minor alarms currently detected by the NCS. Hover your mouse cursor over the Alarm Summary, and the alarm details are displayed as shown in Figure 5-6.

Figure 5-6 NCS Alarm Summary



Note The alarms that appear in the Alarm Summary and Monitor > Alarms pages depend on the settings you specify in the Administration > Settings page. By default, acknowledged alarms are not shown. See the "Modifying Alarm Settings" section on page 5-139 for more information.

Alarms are color coded as follows:

- Red—Critical Alarm
- Orange—Major Alarm
- Yellow—Minor Alarm

Alarms indicate the current fault or state of an element, and alarms are usually generated by one or more events. The alarm can be cleared but the event remains. See the "Alarms and Events Overview" section on page 5-132 for more information about alarms.

Note By default, alarm counts refresh every minute. You can modify when alarms are refreshed in the Administration > User Preferences page.

When you hover your mouse cursor over the Alarm Summary, a pop-up page appears listing the number of critical, major, and minor alarms for each of alarm category. You can specify which alarm categories are displayed in the Alarm Summary on the Administration > User Preferences page. By default, all categories are displayed:

- Alarm Summary—Displays a summary of the total alarms for all alarm categories.
- AP—Display counts for AP alarms such as AP Disassociated from controller, Thresholds violation for Load, Noise or Interference, AP Contained as Rogue, AP Authorization Failure, AP regulatory domain mismatch, or Radio card Failure.
- Context Aware Notifications
- Controller—Displays counts for controller alarms, such as reachability problems from the NCS and other controller failures (fan failure, POE controller failure, AP license expired, link down, temperature sensor failure, and low temperature sensed).
- Coverage Hole—Displays counts for coverage hole alarms generated for access points whose clients are not having enough coverage set by thresholds. See the "Monitoring Maps" section on page 4-1 for more information.
- Mesh Links—Displays counts for mesh link alarms, such as poor SNR, console login, excessive parent change, authorization failure, or excessive association failure.
- Mobility Services—Displays counts for location alarms such as reachability problems from the NCS and location notifications (In/Out Area, Movement from Marker, or Battery Level).
- NCS—Displays counts for the NCS alarms.
- Performance—Displays counts for performance alarms.
- Rogue AP—Displays counts for malicious rogue access points alarms.
- Rogue Adhoc—Displays counts for unclassified rogue access point alarms.
- Security—Displays counts for security alarms such as Signature Attacks, AP Threats/Attacks, and Client Security Events.
- Switch—Displays counts for switch alarms such as authentication errors.

Modifying Alarm Settings

You can modify the following settings for alarms:

- Alarm count refresh rate—See the "Modifying Alarm Count Refresh Rate" section on page 5-139.
- Alarm severity levels—See the "Configuring Alarm Severity Levels" section on page 5-139.

Modifying Alarm Count Refresh Rate

By default, alarm counts refresh every minute. You can modify the refresh rate by selecting **Administration > User Preferences**, and then choosing a new value for the Refresh Alarm Count from the Alarm Summary Every menu.

Configuring Alarm Severity Levels

The Administration > Settings > Severity Configuration page allows you to change the severity level for newly generated alarms.

Note Existing alarms remain unchanged.

To reconfigure the severity level for a newly generated alarm, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Severity Configuration**.

Step 3 Select the check box of the alarm condition whose severity level you want to change.

Step 4 From the Configure Security Level drop-down list, choose from the following severity levels:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Informational**
- **Reset to Default**

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the change or **Cancel** to leave the security level unchanged.

Working with Alarms

You can view, assign, and clear alarms and events on access points and mobility services engine using the NCS.

This section also describes how to have e-mail notifications of alarms sent to you and contains the following topics:

Assigning and Unassigning Alarms

To assign and unassign an alarm to yourself, follow these steps:

Step 1 Perform an advanced search for access point alarms. See the "Advanced Search" section on page 2-34 for more information.

Step 2 Select the alarms that you want to assign to yourself by selecting their corresponding check boxes.

Note To unassign an alarm assigned to you, Unselect the check box next to the appropriate alarm. You cannot unassign alarms assigned to others.

Step 3 From the Select a command drop-down list, choose **Assign to Me** (or **Unassign**), and click **Go**.

If you choose Assign to Me, your username appears in the Owner column. If you choose Unassign, the username column is empty.

Deleting and Clearing Alarms

To delete or clear an alarm from a mobility services engine, follow these steps:

Step 1 In the Monitor > Alarms page, select the alarms that you want to delete or clear by selecting their corresponding check boxes.

Note If you delete an alarm, the NCS removes it from its database. If you clear an alarm, it remains in the NCS database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.

Step 2 From the Select a command drop-down list, choose **Delete** or **Clear**, and click **Go**.

Note To set up cleanup of old alarms and cleared alarms, choose **Administration > Settings > Alarms**. See the "Configuring Alarms" section on page 15-51 for more information.

Acknowledging Alarms

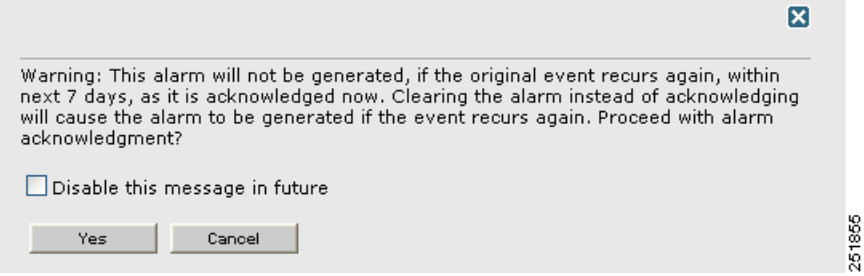
You might want certain alarms to be removed from the Alarms List. For example, if you are continuously receiving an interference alarm from a certain access point on the 802.11g interface, you might want to stop that access point from being counted as an active alarm on the Alarm Summary page or any alarms list. In this scenario, you can find the alarm for the 802.11g interface in the Alarms list, select the check box, and choose **Acknowledge** from the Select a command drop-down list.

Now if the access point generates a new violation on the same interface, the NCS does not create a new alarm, and the Alarm Summary page shows no new alarms. However, if the interference violation is created on another interface, such as 802.11a, a new alarm is created.

By default, acknowledged alarms are not displayed in either the Alarm Summary page or any alarm list page. Also, no e-mail messages generated for these alarms after you have marked them as acknowledged. By default, acknowledged alarms are not included for any search criteria. To change this default, choose to the **Administration > Settings > Alarms** page and unselect the **Hide Acknowledged Alarms** check box.

When you acknowledge an alarm, the following warning appears as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled (see Figure 5-7).

Figure 5-7 Alarm Warning



Note When you acknowledge an alarm, a warning displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Choose **Administration > User Preferences** page to disable this warning message.

You can also search for all previously acknowledged alarms to reveal the alarms that were acknowledged during the last seven days. The NCS automatically deletes cleared alerts that are more than seven days old so your results can only show activity for the last seven days. Until an existing alarm is deleted, a new alarm cannot be generated for any managed entity for which the NCS has already generated an alarm.

Monitoring Access Point Alarms

The Access Point Alarms page displays the access point based alarms on your network.

To access the AP alarms page, do one of the following:

- Perform a search for AP alarms. See the "Using the Search Feature" section on page 2-33 for more information.
- Click the **Access Point** number link in the Alarm Summary box.

The Monitor AP Alarms page contains the following fields:

- Severity—Indicates the severity of the alarm including the following icons.

Icon	Meaning
	Critical
	Major
	Minor
	Warning

Icon	Meaning
	Info
	Unknown **Note** When the controller goes down, the controller inventory dashlet shown the controller status as critical. But the radio inventory dashlet, retains the last known status. In Monitor > AP page, the AP alarm status is shown as "Unknown".
	Clear—Displays if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from the NCS after 30 days.

- Failure Source—Device that generated the alarm.
- Owner—Name of the person to which this alarm is assigned, or blank.
- Date/Time—The time at which the alarm was generated.
- Message—The associated message displayed in the NCS alarm browser.
- Category—Indicates the category assigned to the alarm such as rogue AP, controller, switch, and security.
- Condition—Condition that caused the alarm.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user. See the "Acknowledging Alarms" section on page 5-141 for more information.

Monitoring Air Quality Alarms

The Air Quality Alarms page displays air quality alarms on your network.

To access the air quality alarms page, do one of the following:

- Perform a search for Performance alarms. See the "Using the Search Feature" section on page 2-33 for more information.
- Click the **Performance number** link in the Alarm Summary box.

The Monitor Air Quality Alarms page contains the following fields:

- Severity—Indicates the severity of the alarm including the following icons.

Icon	Meaning
	Critical
	Major

Icon	Meaning
	Minor
	Warning
	Info
	Clear—Appears if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from the NCS after 30 days.

- Failure Source—Device that generated the alarm.
- Owner—Name of the person to which this alarm is assigned, or blank.
- Date/Time—The time at which the alarm was generated.
- Message—The associated message displayed in the NCS alarm browser.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user. See the "Acknowledging Alarms" section on page 5-141 for more information.

Select a command Menu

Select one or more alarms by selecting their respective check boxes, choose one of the following commands from the Select a command drop-down list, and click **Go**.

- **Assign to me**—Assign the selected alarm(s) to the current user.
- **Unassign**—Unassign the selected alarm(s).
- **Clear**—Clear the selected alarm(s).
- **Delete**—Delete the selected alarm(s).
- **Acknowledge**—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See the "Acknowledging Alarms" section on page 5-141 for more information.

Note The alarm remains in the NCS and you can search for all Acknowledged alarms using the alarm search functionality.

- **Unacknowledge**—Unacknowledge an already acknowledged alarm.
- **Email Notification**—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications. See the "Monitoring RFID Tags" section on page 5-118 for more information.

Monitoring CleanAir Security Alarms

The CleanAir Security Alarms page displays security alarms on your network.

To access the security alarms page, do one of the following:

- Perform a search for Security alarms. See the "Using the Search Feature" section on page 2-33 for more information.
- Click the **Security number** link in the Alarm Summary box.

The Monitor CleanAir Security Alarms page contains the following fields:

- Severity—Indicates the severity of the alarm including the following icons:

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info
	Clear—Appears if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from the NCS after 30 days.

- Failure Source—Device that generated the alarm.
- Owner—Name of the person to which this alarm is assigned, or blank.
- Date/Time—The time at which the alarm was generated.
- Message—The associated message displayed in the NCS alarm browser.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user. See the "Acknowledging Alarms" section on page 5-141 for more information.

Select a command Menu

Select one or more alarms by selecting their respective check boxes, choose one of the following commands from the Select a command drop-down list, and click **Go**.

- **Assign to me**—Assign the selected alarm(s) to the current user.
- **Unassign**—Unassign the selected alarm(s).
- **Clear**—Clear the selected alarm(s).
- **Delete**—Delete the selected alarm(s).
- **Acknowledge**—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See the "Acknowledging Alarms" section on page 5-141 for more information.

Note The alarm remains in the NCS and you can search for all Acknowledged alarms using the alarm search functionality.

- **Unacknowledge**—Unacknowledge an already acknowledged alarm.
- **Email Notification**—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications. See the "Monitoring RFID Tags" section on page 5-118 for more information.

Monitoring Email Notifications

The NCS includes a built-in e-mail notification function which can notify the network operator when critical alarms occur.

The Email Notification page allows you to add a filter for each alert category. The severity level is set to critical by default when the alert category is enabled, but you can choose a different severity level for different categories. E-mail notifications are generated only for the severity levels that are configured.

To configure e-mail notifications, follow these steps:

Step 1 Choose **Monitor > Alarms**.

Step 2 From the Select a command drop-down list, choose **Email Notification**.

Step 3 Click **Go**.

Step 4 Click an Alarm Category to edit severity level and e-mail recipients for its e-mail notifications.

Step 5 Select the severity level check box(es) (Critical, Major, Minor, or Warning) for which you want a notification sent.

Step 6 Enter the notification recipient e-mail addresses in the To text box.

Note Separate multiple e-mail addresses with a comma.

Step 7 Click **OK**.

Step 8 Select the **Enabled** check box for applicable alarm categories to activate the delivery of e-mail notifications.

Step 9 Click **OK**.

Monitoring Severity Configurations

You can change the severity level for newly generated alarms.

Note Existing alarms remain unchanged.

To change the severity level of newly-generated alarms, follow these steps:

Step 1 Choose **Administration > Setting**.

Step 2 Choose **Severity Configuration** from the left sidebar menu.

Step 3 Select the check box of the alarm condition for which you want to change the severity level.

Step 4 From the Configure Severity Level drop-down list, choose the new severity level (Critical, Major, Minor, Warning, Informational, Reset to Default).

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the change.

Monitoring Cisco Adaptive wIPS Alarms

Alarms from Cisco Adaptive wIPS DoS (denial of service) and security penetration attacks are classified as security alarms. You can view these wIPS alarms and their details in the Monitor > Alarms page.

To view a list of wIPS DoS and security penetration attack alarms, follow these steps:

Step 1 Perform a search for Security alarms using the Advanced Search feature. See the "Advanced Search" section on page 2-34 for more information on performing an advanced search.

The following information is provided for wIPS alarms:

- Severity—Severity levels include critical, major, info, warning, and clear.
- Failure Object—Displays the name and IP or MAC address of the object for which the alarm was generated. Click the Failure Object to view alarm details. See the "Monitoring Cisco Adaptive wIPS Alarm Details" section on page 5-148 for more information on viewing wIPS alarm details.
- Date/Time—Displays the date and time that the alarm occurred.
- Message—Displays a message explaining why the alarm occurred (such as the applicable wIPS policy).
- Acknowledged—Displays whether or not the alarm is acknowledged by the user.
- Category—Indicates the category of this alarm such as Security.
- Condition—Displays a description of what caused this alarm to be triggered.

When there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

To add, remove, or reorder columns in the table, click the **Edit View** link to go to the Edit View page.

Select a command

Using the Select a command drop-down list, you can perform the following actions on the selected alarms:

- **Assign to me**—Assign the selected alarm(s) to the current user.
- **Unassign**—Unassign the selected alarm(s).
- **Delete**—Delete the selected alarm(s).
- **Clear**—Clear the selected alarm(s).

- **Acknowledge**—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the NCS and you can search for all Acknowledged alarms using the alarm search functionality.
- **Unacknowledge**—You can choose to unacknowledge an already acknowledged alarm.
- **Email Notification**—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications.

To perform an action on the selected alarm, follow these steps:

Step 1 Select an alarm by selecting its check box.

Step 2 From the Select a command drop-down list, select the applicable command.

Step 3 Click **Go**.

Monitoring Cisco Adaptive wIPS Alarm Details

Choose **Monitor > Alarms >** *failure object* to view details of the selected Cisco wIPS alarm. The following Alarm details are provided for Cisco Adaptive wIPS alarms:

- General
  - Detected By wIPS AP—The access point that detected the alarm.
  - wIPS AP IP Address—The IP address of the wIPS access point.
  - Owner—Name of person to which this alarm is assigned or left blank.
  - Acknowledged—Displays whether or not the alarm is acknowledged by the user.
  - Category—For wIPS, the alarm category is Security.
  - Created—Month, day, year, hour, minute, second, AM or PM that the alarm was created.
  - Modified—Month, day, year, hour, minute, second, AM or PM that the alarm was last modified.
  - Generated By—Indicates how the alarm event was generated (either NMS or from a trap).

    NMS (Network Management System - NCS)—Generated through polling. The NCS periodically polls the controllers and generates events. The NCS generates events when the traps are disabled or when the traps are lost for those events. In this case, “Generated by” is NMS.

    Trap—Generated by the controller. The NCS process these traps and raises corresponding events for them. In this case, “Generated by” is Controller.
  - Severity—Level of severity including critical, major, info, warning, and clear.
  - Last Disappeared—The date and time that the potential attack last disappeared.
  - Channel—The channel on which the potential attack occurred.
  - Attacker Client/AP MAC—The MAC address of the client or access point that initiated the attack.
  - Attacker Client/AP IP Address—The IP address of the client or access point that initiated the attack.
  - Target Client/AP IP Address—The IP address of the client or access point targeted by the attacker.
  - Controller IP Address—The IP address of the controller to which the access point is associated.

  - MSE—The IP address of the associated mobility services engine.
  - Controller MAC address—The MAC address of the controller to which the access point is associated.
  - wIPS access point MAC address
  - Forensic File
  - Event History—Takes you to the "Monitoring Alarms" page to view all events for this alarm.
- Annotations—Enter any new notes in this text box, and click **Add** to update the alarm. Notes are displayed in the "Annotations" display area.
- Messages—Displays information about the alarm.
- Audit Report—Click to view config audit alarms details. This report is only available for Config Audit alarms.

  Configuration audit alarms are generated when audit discrepancies are enforced on config groups.

  Note If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group.
  The alarms have links to the audit report where you can view a list of discrepancies for each controller.

- Rogue Clients—If the failure object is a rogue access point, information about rogue clients is displayed.

Select a command

Select one or more alarms by selecting their respective check boxes, and click **Go**.

- **Assign to me**—Assign the selected alarm(s) to the current user.
- **Unassign**—Unassign the selected alarm(s).
- **Delete**—Delete the selected alarm(s).
- **Clear**—Clear the selected alarm(s).
- **Acknowledge**—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the NCS and you can search for all Acknowledged alarms using the alarm search functionality.
- **Unacknowledge**—You can choose to unacknowledge an already acknowledged alarm.
- **Email Notification**—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications.
- **Event History**—Takes you to the Monitor Alarms > Events page to view events for Rogue Alarms.

Monitoring Events

One or more events might generate an abnormal state or alarm. The alarm can be cleared, but the event remains. Choose **Monitor > Events** to access the Events page, which displays the following information:

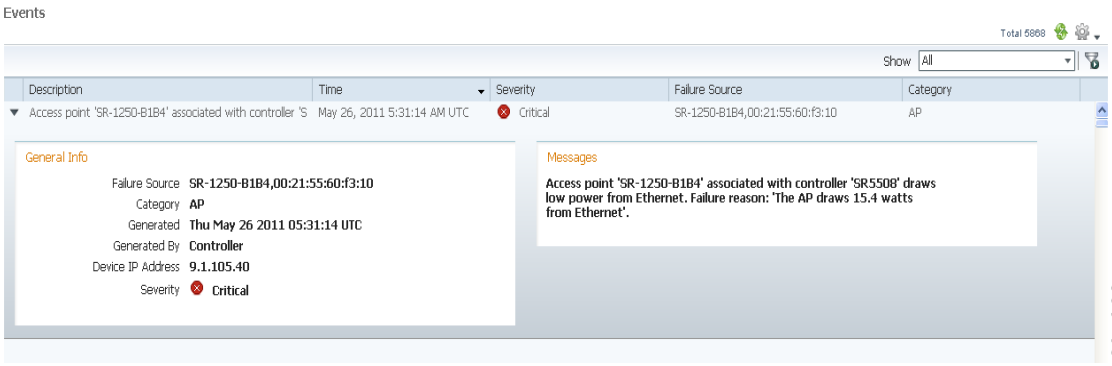
- Description—Describes the event details.
- Time—Indicates the date and time the event was generated.

- Severity—Event severities include: Critical, Major, Minor, Warning, Cleared, or Information.
- Failure Source—Indicates the source of the event (including name and/or MAC address).
- Category—Type of event such as Rogue AP, Security, or AP.

Click any column heading to sort by that column.

Use the quickview icon to disclose more information on the event. The additional information for the event is divided into general information and the message. In the general information, the failure source, the category, severity, generated time and IP address. The message of the event is also displayed (See Figure 5-8).

Figure 5-8 Viewing Events



Note Events also has preset, quick and advanced filters similar to alarms. These filters work in same way as the filters in alarms.

When you filter the table using the Search feature, the Events page might display the additional information. See the "Advanced Search" section on page 2-34(Advanced Search results for Events) for more information on performing a search. The additional information includes the following:

- Coverage Hole Events
  - Access Point Name
  - Failed Clients—Number of clients that failed due to the coverage hole.
  - Total Clients—Total number of clients affected by the coverage hole.
  - Radio Type—The radio type (802.11b/g or 802.11a) of the applicable access point.
  - Coverage Threshold
- Rogue AP Events
  - Vendor—Rogue access point vendor name or Unknown.
  - Classification Type—Indicates the type of rogue access point including Malicious, Friendly, or Unclassified.
  - On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
  - Radio Type—Lists all radio types applicable to this rogue access point.

  - State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
  - SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Note See the "Monitoring Rogue Alarm Events" section on page 5-113 or the "Viewing Rogue AP Event Details" section on page 5-114 for more information on rogue access points events.

- Adhoc Rogue Events
  - Vendor—Rogue access point vendor name or Unknown.
  - On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
  - Radio Type—Lists all radio types applicable to this rogue access point.
  - State—Indicates the state of the alarm. Possible states for ad hoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
  - SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Interference
  - Detected By—IP address of the device that detected the interference.
  - ID—ID of the device that detected the interference.
- Mesh Links
- Client
- Context Aware Notification
- Pre Coverage Hole
  - Client MAC Address—MAC address of the client affected by the Pre Coverage Hole.
  - AP MAC Address—MAC address of the applicable access point.
  - Radio Type—The radio type (802.11b/g or 802.11a) of the applicable access point.
  - Power Level—Access Point transmit power level (1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, 5 = 0.195 to 6.25% power).
  - Client Type—Client type can be laptop(0), pc(1), pda(2), dot11mobilephone(3), dualmodephone(4), wgb(5), scanner(6), tabletpc(7), printer(8), projector(9), videoconfsystem(10), camera(11), gamingsystem(12), dot11deskphone(13), cashregister(14), radiotag(15), rfidsensor(16), server(17)
  - WLAN Coverage Hole Status

If there is more than one page of events, the number of pages is displayed with a scroll arrow on each side. Use this to view additional events.

This section contains the following topics:

Searching Events

Use the NCS Search feature to find specific events or to create and save custom searches. See one of the following topics for additional information:

- Using the Search Feature, page 2-33
- Quick Search, page 2-33
- Advanced Search, page 2-34
- Saved Searches, page 2-46

Exporting Events

You can quickly export the list of events into a CSV file (a spreadsheet format with comma-separated values).

Note The columns that are shown in the events table are only exported to the CSV file.

To export the list of events, follow these steps:

Step 1 Choose **Monitor > Events**.

Step 2 Click the icon on the toolbar. A pop-up window appears.

Step 3 In the File Download window, click **Save** to save the file.

Monitoring Failure Objects

Note The event categories Location Servers and Location Notifications appear only in the Cisco NCS Location version.

Choose **Monitor > Events**, then click the expand icon to the far left of the Monitor > Events page for the event for which you want to see details. Details about the event are displayed. Depending on the type of event you selected, the associated details vary.

- General Info
  - Failure Source—Indicates the source of the event (including name and/or MAC address).

  - Category—Type of alarm such as Security or AP.
  - Generated—Date and time that the event was generated.
  - Generated By—Indicates how the alarm event was generated (either NMS or from a trap).

    NMS (Network Management System - NCS)—Generated through polling. The NCS periodically polls the controllers and generates events. The NCS generates events when the traps are disabled or when the traps are lost for those events. In this case, "Generated by" is NMS.

    Trap—Generated by the controller. The NCS process these traps and raises corresponding events for them. In this case, "Generated by" is Controller.
  - Device IP Address—IP address of the alarm-generating device.
  - Severity—Level of severity including critical, major, info, warning, and clear.
- Messages—Message explaining why the event occurred.

Monitoring Events for Rogue APs

Choose **Monitor > Events**. Click an item in the Description column to display the alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by controllers. The following fields appear:

General

- Rogue MAC Address
- Vendor
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Owner—Name of person to which this alarm is assigned, or (blank).
- State—State of this radio relative to the network or Port. Rogue access point radios appear as "Alert" when first scanned by the Port, or as "Pending" when operating system identification is still underway.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Containment Level—An access point which is being contained is either unable to provide service at all, or provides exceedingly slow service. There is a level associated with the containment activity which indicates how many Cisco 1000 series lightweight access points to use in containing the threat. This service must be initiated and halted by the administrator. Containment Type - Contained if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status, otherwise Unassigned.
- Channel—Indicates the band at which the ad hoc rogue is broadcasting.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Created—Date and time that the event occurred.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  - NMS (Network Management System - NCS)—Generated through polling. The NCS periodically polls the controllers and generates events. The NCS generates events when the traps are disabled or when the traps are lost for those events. In this case, "Generated by" is NMS.

  - Trap—Generated by the controller. The NCS process these traps and raises corresponding events for them. In this case, "Generated by" is Controller.
- Device IP Address—IP address of the alarm-generating device.
- Severity—Level of severity, Critical, Major, Minor, Warning, Clear, Info. Color coded.

Message—Displays descriptive information about the alarm.

Help—Displays information about the alarm.

Note Use the Advance Search feature to find specific events. See the "Advanced Search" section on page 2-34 for more information.

Monitoring Events for Ad hoc Rogues

Choose **Monitor > Events**. Click an item in the Description column to display ad hoc rogue event details.

General

- Rogue MAC Address
- Vendor
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Owner—Name of person to which this alarm is assigned, or (blank).
- State—State of this radio relative to the network or Port. Rogue access point radios appear as "Alert" when first scanned by the Port, or as "Pending" when operating system identification is still underway.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Containment Level—An access point which is being contained is either unable to provide service at all, or provides exceedingly slow service. There is a level associated with the containment activity which indicates how many Cisco 1000 series lightweight access points to use in containing the threat. This service must be initiated and halted by the administrator. Containment Type - Contained if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status, otherwise Unassigned.
- Channel—Indicates the band at which the ad hoc rogue is broadcasting.
- Created—Date and time that the event occurred.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  - NMS (Network Management System - NCS)—Generated through polling. The NCS periodically polls the controllers and generates events. The NCS generates events when the traps are disabled or when the traps are lost for those events. In this case, "Generated by" is NMS.

  - Trap—Generated by the controller. The NCS process these traps and raises corresponding events for them. In this case, "Generated by" is Controller.
- Device IP Address—IP address of the alarm-generating device.
- Severity—Level of severity, Critical, Major, Minor, Warning, Clear, Info. Color coded.

Message—Displays descriptive information about the alarm.

Help—Displays information about the alarm.

Monitoring Cisco Adaptive wIPS Events

Choose **Monitor > Events** to view wIPS events. One or more events might generate an abnormal state or alarm. The alarm can be cleared, but the event remains. For more information regarding monitoring events, see the "Monitoring Events" section on page 5-149.

The following sections provide additional information regarding Cisco Adaptive wIPS:

- Configuring wIPS Profiles
- NCS Services
- wIPS Policy Alarm Encyclopedia

Perform an events search to narrow the results to mobility services engine or Security events only. To view mobility services engine or Security events, choose **Monitor > Events**.

Note If there is more than one page of events, the number of pages is displayed with a scroll arrow on each side. Use this to view additional events.

Monitoring CleanAir Air Quality Events

You can use the NCS to view the events generated on the air quality of the wireless network.

To view air quality events, follow these steps:

Step 1 Click **Advanced Search** in the NCS.

The New Search page appears.

Step 2 In the New Search page, choose **Events** from the Search Category drop-down list.

Step 3 From the Severity drop-down list, choose the type of severity you want to search the air quality events.

Step 4 From the Event Category drop-down list, choose *Performance*.

Step 5 Click **Go**.

The air quality events page displays the following information:

- Severity—Indicates the severity of the alarm including the following icons.

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info
	Clear—Appears if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from the NCS after 30 days.

- Failure Source—Device that generated the alarm.
- Date/Time—The time at which the alarm was generated.

Viewing Air Quality Event Details

To view air quality event details, follow these steps:

Step 1 From the Air Quality Events page, click an item under Failure Source to access the alarm details page. See the "Monitoring CleanAir Air Quality Events" section on page 5-155.

Step 2 The air quality event page displays the following information:

- Failure Source—Device that generated the alarm.
- Category—The category this event comes under. In this case, Performance.
- Created—The time stamp at which the event was generated.
- Generated by—The device that generated the event.
- Device IP Address—The IP address of the device that generated the event.
- Severity—The severity of the event.
- Alarm Details—A link to the related alarms associated with this event. Click the link to learn more about the alarm details.
- Message—Describes the air quality index on this access point.

Monitoring Interferer Security Risk Events

You can use the NCS to view the security events generated on your wireless network.

To view interferer security events, follow these steps:

Step 1 Click **Advanced Search** in the NCS.

The New Search page appears.

Step 2 In the New Search page, choose **Events** from the Search Category drop-down list.

Step 3 From the Severity drop-down list, choose the type of severity you want to search the air quality events.

Step 4 From the Event Category drop-down list, choose **Security**.

Step 5 Click **Go**.

The interferer security events page displays the following information:

- Severity—Indicates the severity of the alarm including the following icons.

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info
	Clear—Appears if the rogue is no longer detected by any access point. **Note** Rogues can be detected by multiple access points. If one access point no longer detects the rogue but the other access point does, Clear is not sent. **Note** Once the severity of a rogue is Clear, the alarm is deleted from the NCS after 30 days.

- Failure Source—Device that generated the alarm.
- Date/Time—The time at which the alarm was generated.

Viewing Interferer Security Risk Event Details

To view interferer security event details, follow these steps:

Step 1 In the Interferer Security Event details page, click an item under Failure Source to access the alarm details page. See the "Monitoring Interferer Security Risk Events" section on page 5-156.

Step 2 The air quality event page displays the following information:

- Failure Source—Device that generated the alarm.
- Category—The category this event comes under. In this case, Security.

- Created—The time stamp at which the event was generated.
- Generated by—The device that generated the event.
- Device IP Address—The IP address of the device that generated the event.
- Severity—The severity of the event.
- Alarm Details—A link to the related alarms associated with this event. Click the link to know more about the alarm details.
- Message—Describes the interferer device affecting the access point.

Monitoring Health Monitor Events

You can use the NCS to view the events generated by the Health Monitor.

To view the health monitor events, follow these steps:

Step 1 Click **Advanced Search** in the NCS.

The New Search page appears.

Step 2 In the New Search page, choose **Events** from the Search Category drop-down list.

Step 3 From the Severity drop-down list, choose the type of severity you want to search the health monitor events.

Step 4 From the Event Category drop-down list, choose **the NCS**.

Step 5 Click **Go**.

The Health Monitor Events page displays the following information:

- Severity—Indicates the severity of the alarm including the following icons.

Icon	Meaning
	Critical
	Major
	Minor
	Warning
	Info
	Clear

- Failure Source—Device that generated the alarm.
- Date/Time—The time at which the alarm was generated.
- Message—Describes the health details.

Viewing Health Monitor Event Details

To view health monitor event details, follow these steps:

Step 1 In the Health Monitor Events page, click an item under Failure Source to access the alarm details page. See the "Monitoring Health Monitor Events" section on page 5-158.

Step 2 The Health Monitor Events page displays the following information:

- Failure Source—Device that generated the alarm.
- Category—The category this event comes under. In this case, NCS.
- Created—The time stamp at which the event was generated.
- Generated by—The device that generated the event.
- Device IP Address—The IP address of the device that generated the event.
- Severity—The severity of the event.
- Alarm Details—A link to the related alarms associated with this event. Click the link to know more about the alarm details.
- Message—Describes the event through a message.

Working with Events

You can use the NCS to view mobility services engine and access point events. You can search and display events based on their severity (critical, major, minor, warning, clear, info) and event category or you can search for a mobility services engine and access point by its IP address, MAC address or name.

A successful event search displays the event severity, failure object, date and time of the event, and any messages for each event.

To display events, follow these steps:

Step 1 In the NCS, click **Monitor > Events**.

Step 2 In the Events page:

- If you want to display the events for a specific element and you know its IP address, MAC address, or Name, enter that value in the Quick Search text box (left pane). Click **Go**.
- To display events by severity and category, choose the appropriate options from the Severity and Event Category drop-down lists (left pane). Click **Search**.

Step 3 If the NCS finds events that match the search criteria, it displays a list of these events.

Note For more information about an event, click the failure object associated with the event. Additionally, you can sort the events summary by each of the column headings.

Monitoring Site Maps

Maps provide a summary view of all your managed systems on campuses, buildings, outdoor areas, and floors. With the NCS database, you can add maps and view your managed system on realistic campus, building, and floor maps. See the "Monitoring Maps" section on page 4-1 for more information.

Monitoring Google Earth Maps

You can enable location presence by mobility server to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by clients on a demand basis for use by location-based services and applications. Location Presence can be configured when a new campus, building, floor, or outdoor area is being added or configured at a later date. See the "Monitoring Google Earth Maps" section on page 4-112 for more information.

CHAPTER 4

Monitoring Maps

This chapter describes how to add maps to the Cisco NCS database and use them to monitor your LAN. With the NCS database, you can add maps and view your managed system on realistic campus, building, and floor maps.

Note Additionally, you can enable location presence by mobility server to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by clients on a demand basis for use by location-based services and applications. Location presence can be configured when a new campus, building, floor, or outdoor area is being added or configured at a later date.

Note A mobility server should be synchronized before location presence is enabled. For details on enabling location presence and assigning its parameters, see the *Cisco Context-Aware Services documentation*. This configuration guide also covers verifying location accuracy, using chokepoints, using Wi-FI TDOA receivers, applying calibration models, and other context-aware planning and verification topics.

This chapter contains the following sections:

Information About Maps

This section contains the following topics:

Maps

Maps provide a summary view of all your managed systems on campuses, buildings, outdoor areas, and floors. The available information includes the following:

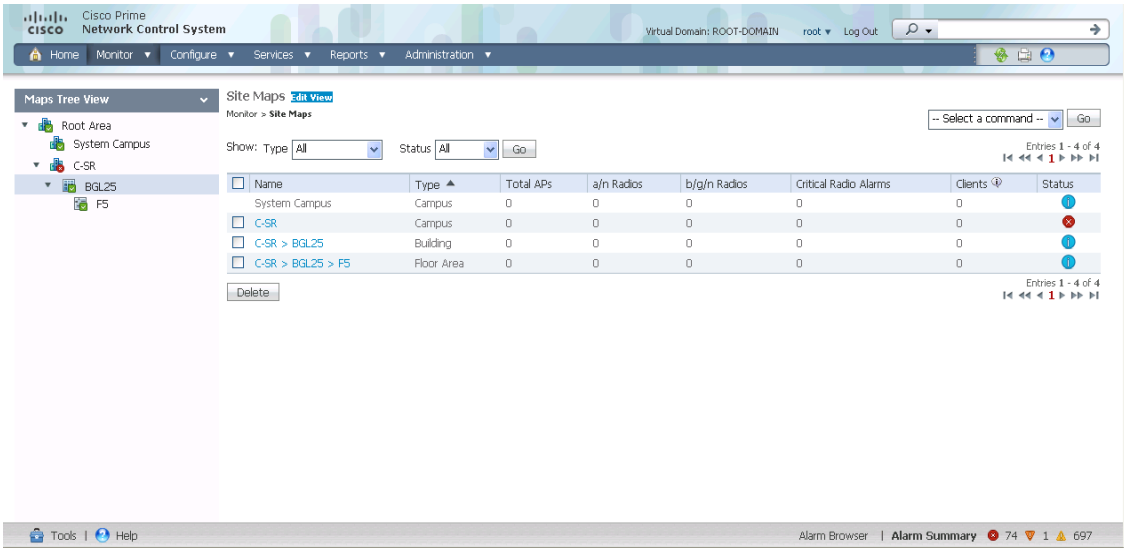
- Total APs—Number of total access points for each map.
- 802.11a/n Radios and 802.11b/g/n Radios—Number of 802.11a/n and 802.11b/g/n radios associated with each map.
- Out of Service (OOS) Radios—Number of 802.11a/n and 802.11b/g/n radios associated with each map.
- Clients—Number of clients associated to access points on the map.
- AP Heat Maps—A real-time wireless RF graphical representation of data which shows RF coverage throughout a facility or campus through the use of a heat map. For more information on Heat APs see the "Understanding RF Heatmap Calculation" section on page 4-110.

Note This number is based on the most recent client statistics poll. The number of clients located on the map by MSE might not match this number.

- 802.11a/n and 802.11b/g/n Avg Air Quality—Indicates the average Air Quality (AQ) for 802.11a/n and 802.11b.g.n radios.
- 802.11a/n and 802.11b/g/n Min Air Quality—Indicates the minimum Air Quality (AQ) for 802.11a/n and 802.11b/g/n radios.
- Status—Indicates the current status of the map.
  - Red circle—Critical fault
  - Yellow triangle—Minor fault
  - Green square—Ok

Note To view or edit current maps, choose **Monitor > Site Maps** (see Figure 4-1), and choose the appropriate map from the list. Use the Select a command drop-down list to access additional functionality.

Figure 4-1 Site Maps Page



The left sidebar menu lists all campuses, buildings, and floors in a tree view. When you click a campus, building, or floor in the Maps Tree View menu, the main area of the page displays corresponding information.

Note Click **Edit View** to change the information displayed for the listed maps. See the "Configuring Edit View" section on page 4-9 for more information.

Note The Root area (listed in the Maps Tree View menu) displays a list of buildings that are not in campuses. Status and object counts for root area buildings are not aggregated.

Use the Select a command drop-down list for additional map functionality.

Campus

A campus is the area in which a building, an outdoor area, or set of surrounding buildings are situated.

Building

A structure that has a roof and walls and stands more or less permanently in one place.

Floor Area

The floor area is the area of each floor of the building measured to the outer surface of the outer walls including the area of lobbies, cellars, elevator shafts, and in multi-dwelling buildings, all the common spaces.

Outdoor Area

An area that includes a building or set of buildings, or could be just plain land that is not an indoor area.

Access Points

Access points (APs) are specially configured nodes on wireless local area networks (WLANs). Access points act as a central transmitter and receiver of WLAN radio signals. Access points support Wi-Fi wireless communication standards.

Chokepoints

Installation of chokepoints provides enhanced location information for RFID tags. When an active Cisco Compatible Extensions version 1 compliant RFID tag enters the range of a chokepoint, it is stimulated by the chokepoint. The MAC address of this chokepoint is then included in the next beacon sent by the stimulated tag. All access points that detect this tag beacon then forward the information to the controller and location appliance. See the "Configuring ChokePoints" section on page 4-58 for more information.

Wi-Fi TDOA Receivers

TDOA technology uses a time-based method to calculate the location. Each Wi-Fi TDOA receivers report the time of arrival of the signal from the tag to its respective receiver. The mobility services engine correlates the time of arrival for all the tag signals from all the TDOA receivers to find the intersection points of known distances. The greater the number of receivers used in the calculation, the more accurately the tag can be located. Wi-Fi TDOA receivers are typically used for calculating location information in manufacturing or retail warehouse environments (where there are lots of machines or high ceilings or both), in outdoor environments, or in other line-of-site environments. See the "Configuring Wi-Fi TDOA Receivers" section on page 4-61 for more information.

Map Editor

You can use the NCS map editor to define, draw, and enhance floor plan information. The map editor enables you to create obstacles to consider when you compute RF prediction heat maps for access points. You can also add coverage areas for MSEs that locate clients and tags in that particular area.

With the map editor, you can perform the following functions:

- Save—Saves the current map image.
- Recompute prediction—Updates the RF prediction heatmap if any changes are made to the existing floor map image.
- Reload Last Saved—Loads the last saved map image.
- Select all—Selects all the obstacles and coverage areas that you have created.
- Unselect—Deselects the obstacles and coverage areas that are selected.
- Move selected Obstacles—Moves the selected obstacles to a different location on the map.
- Duplicate selected Obstacles—Creates a copy of the selected obstacles.
- Zoom in/Zoom out—Zoom in or out on the image you are currently viewing.

- Show floor image—Use this to display the floor image.
- Show obstacles—Use this to display the obstacles.
- Larger resolution/Medium resolution/Smaller resolution—Increase or decrease the resolution of the floor map image.
- SNAP Mode—Use this to snap an obstacle to its nearest obstacle while drawing.
- ORTHO Mode—Use to draw a horizontal or vertical obstacle. This is especially useful when you want to draw all the obstacles at right angles.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature and contains the following topics:

- Guidelines for Using the Map Editor, page 4-5
- Guidelines for Placing Access Points, page 4-5
- Guidelines for Inclusion and Exclusion Areas on a Floor, page 4-7

Guidelines for Using the Map Editor

Consider the following when modifying a building or floor map using the map editor:

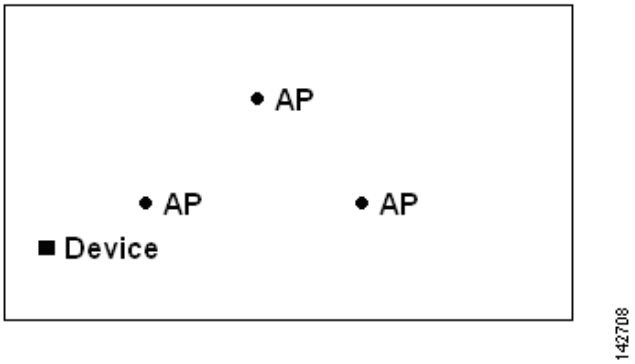
- We recommend that you use the map editor to draw walls and other obstacles rather than importing an .FPE file from the legacy floor plan editor.
  - If necessary, you can still import .FPE files. To do so, navigate to the desired floor area, choose **Edit Floor Area** from the Select a command drop-down list, click **Go**, select the **FPE File** check box, and browse to choose the .FPE file.
- You can add any number of walls to a floor plan with the map editor; however, the processing power and memory of a client workstation might limit the refresh and rendering aspects of the NCS.
  - We recommend a practical limit of 400 walls per floor for machines with 1GB RAM or less.
- All walls are used by the NCS when generating RF coverage heatmaps.
  - However, the MSEs use no more than 50 heavy walls in its calculations, and the MSE does not use light walls in its calculations because those attenuations are already accounted for during the calibration process.

If you have a high resolution image (near 12 megapixels), you might need to scale down the image resolution with an image editing software prior to using map editor.

Guidelines for Placing Access Points

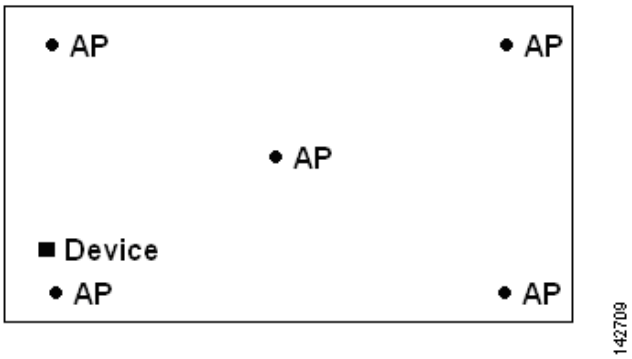
Place access points along the periphery of coverage areas to keep devices close to the exterior of rooms and buildings (see Figure 4-2). Access points placed in the center of these coverage areas provide good data on devices that would otherwise appear equidistant from all other access points.

Figure 4-2 Access Points Clustered Together



By increasing overall access point density and moving access points towards the perimeter of the coverage area, location accuracy is greatly improved (see Figure 4-3).

Figure 4-3 Improved Location Accuracy by Increasing Density



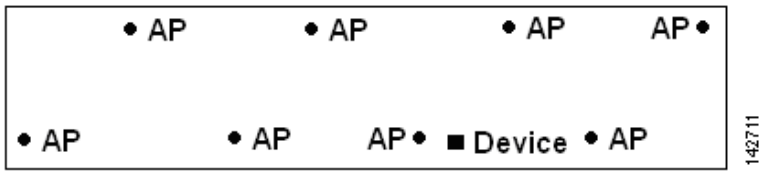
In long and narrow coverage areas, avoid placing access points in a straight line (see Figure 4-4). Stagger them so that each access point is more likely to provide a unique snapshot of a device location.

Figure 4-4 Refrain From Straight Line Placement

Although the design in Figure 4-4 might provide enough access point density for high bandwidth applications, location suffers because each access point view of a single device is not varied enough; therefore, location is difficult to determine.

Move the access points to the perimeter of the coverage area and stagger them. Each has a greater likelihood of offering a distinctly different view of the device, resulting in higher location accuracy (see Figure 4-5).

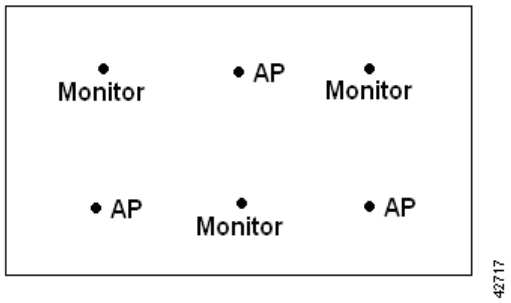
Figure 4-5 Improved Location Accuracy by Staggering Around Perimeter



Most current wireless handsets support only 802.11b/n, which offers only three non-overlapping channels. Therefore, wireless LANs designed for telephony tend to be less dense than those planned to carry data. Also, when traffic is queued in the Platinum QoS bucket (typically reserved for voice and other latency-sensitive traffic), lightweight access points postpone their scanning functions that allow them to peak at other channels and collect, among other things, device location information. The user has the option to supplement the wireless LAN deployment with access points set to monitor-only mode. Access points that perform only monitoring functions do not provide service to clients and do not create any interference. They simply scan the airwaves for device information.

Less dense wireless LAN installations, such as voice networks, find their location accuracy greatly increased by the addition and proper placement of monitor access points (see Figure 4-6).

Figure 4-6 Less Dense Wireless LAN Installations



Verify coverage using a wireless laptop, handheld, or phone to ensure that no fewer than three access points are detected by the device. To verify client and asset tag location, ensure that the NCS reports client devices and tags within the specified accuracy range (10 m, 90%).

Note If you have a ceiling-mounted AP with an integrated omni-directional antenna, the antenna orientation does not really need to be set in the NCS. However, if you mount that same AP on the wall, you must set the antenna orientation to 90 degrees.

Guidelines for Inclusion and Exclusion Areas on a Floor

Inclusion and exclusion areas can be any polygon shape and must have at least three points.

You can only define one inclusion region on a floor. By default, an inclusion region is defined for each floor when it is added to the NCS. The inclusion region is indicated by a solid aqua line, and generally outlines the region.

You can define multiple exclusion regions on a floor.

Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

Monitoring Maps

This section contains the following topics:

Configuring Maps

This section contains the following topics:

Viewing a Map

To view a current campus map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the name of the campus map to view its details in the Campus View page (see Figure 4-7).

Figure 4-7 Campus View

Step 3 The Select a command drop-down list provides the following options:

- New Floor Area—See the "Adding Floor Areas to a Campus Building" section on page 4-28 for more information.
- Edit Building—See the "Editing a Map" section on page 4-10 for more information.
- Delete Building—See the "Deleting a Map" section on page 4-10 for more information.
- Copy Building—See the "Managing RF Calibration Models" section on page 4-64 for more information.
- Edit Location Presence Information—See the "Managing Location Presence Information" section on page 4-70 for more information.

Note Use the **Monitor > Site Maps > Campus View** main navigation bar at the top of the campus image to enlarge or decrease the size of the map view and to hide or show the map grid (which displays the map size in feet or meters).

Configuring Edit View

The Edit View page enables you to choose which columns appear in the maps list page.

Note Name and Type are fixed columns. They cannot be moved or hidden.

Column names appear in one of the following lists:

- Hide Information—Lists columns that do not appear in the table. The Hide button points to this list.
- View Information—Lists columns that do appear in the table. The Show button points to this list.

To display a column in a table, click it in the Hide Information list, then click **Show**. To remove a column from a table, click it in the View Information list, then click **Hide**. You can select more than one column by pressing the Shift or Control key.

To change the position of a column in the View Information list, click it, then click **Up** or **Down**. The higher a column is in the list, the farther left it appears in the table.

Edit View Command Buttons

The Edit View page contains the following command buttons:

- Reset—Sets the table to the default display.
- Show—Moves the highlighted columns from the Hide Information list to the View Information list.
- Hide—Moves the highlighted columns from the View Information list to the Hide Information list.
- Up—Moves the highlighted columns upward in the list (further to the left in the table).
- Down—Moves the highlighted columns downward in the list (further to the right in the table).
- Submit—Saves the changes to the table columns and return to the previous page.
- Cancel—Discards the changes to the table columns and return to the previous page.

Editing a Map

To edit a current campus map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the name of the campus map to open its details page.

Step 3 From the Select a command drop-down list, choose **Edit Campus**.

Step 4 Make any necessary changes to the Campus Name and the Contact.

Note To change the unit of measurement (feet or meters), choose **Monitor > Site Maps** and choose **Properties** from the Select a command drop-down list.

Step 5 Click **Next**.

Step 6 Make any additional changes to Maintain Aspect Ratio or Dimensions (feet).

Step 7 Click **OK**.

Note System Campus is part of all partitions. Also, you cannot edit or delete a system campus.

Deleting a Map

To delete a map, follow these steps:

Step 1 In the Monitor > Site Maps page, Select the check box(es) for the map(s) that you want to delete.

Step 2 Click **Delete** at the bottom of the map list or choose **Delete Maps** from the Select a command drop-down list, and click **Go**.

Step 3 Click **OK** to confirm the deletion.

Note Deleting a campus or building also deletes all of its container maps. The access points from all deleted maps are moved to an Unassigned state. System Campus can not be deleted, however buildings or floors in system campus can be modified.

Copying a Map

The following guidelines apply to the copying process:

- Only the child elements are copied to the new map.
- The selected map is copied to the current applicable partition.
- Overlapping areas are not checked when buildings are copied. You should edit these after copying the map for proper positioning.
- If the selected map is above ground, the first available floor above ground is used for the copy.
- If the selected map is a basement, the first available basement is used for the copy.
- The following are *not* copied:
  - Access points and their positioning coordinates.
  - Planning mode data.

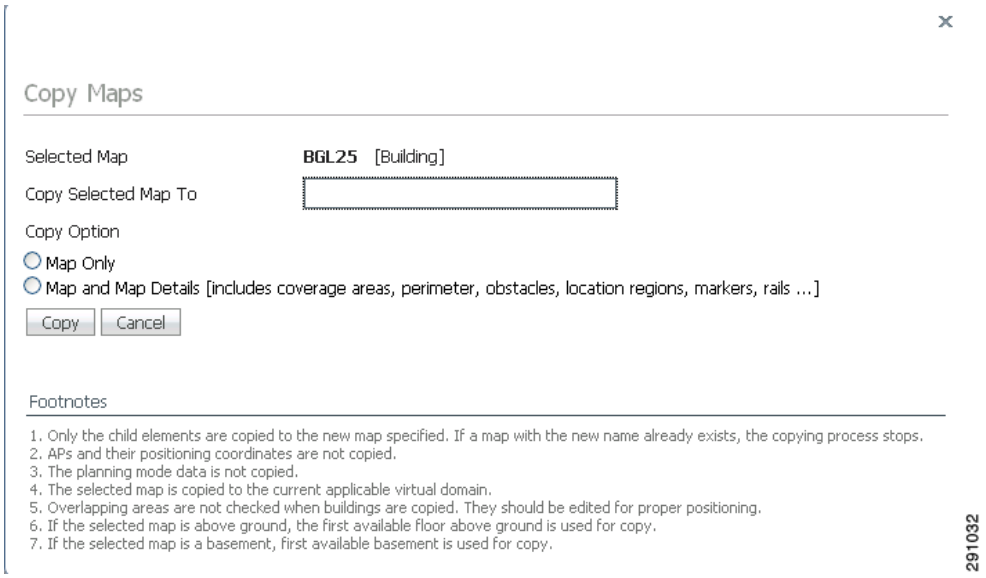
Note You cannot copy a System Campus.

To copy a map, follow these steps:

Step 1 In the Monitor > Site Maps page, select the check box of the map that you want to copy.

Step 2 From the Select a command drop-down list, choose **Copy Maps**. The Copy Maps dialog box appears (see Figure 4-8).

Figure 4-8 Copy Maps



Step 3 Enter the name of the new map to which you want to copy the current map.

Note If a map with the new name already exists, the copying process stops.

Step 4 Select the Copy Option (**Map Only** or **Map and Map Details**) radio button.

Note Map and Map Details includes coverage areas, perimeters, obstacles, location regions, markers, and rails.

Step 5 Click **Copy** to complete the copying process or **Cancel** to close the dialog box without copying the current map.

Exporting a Map

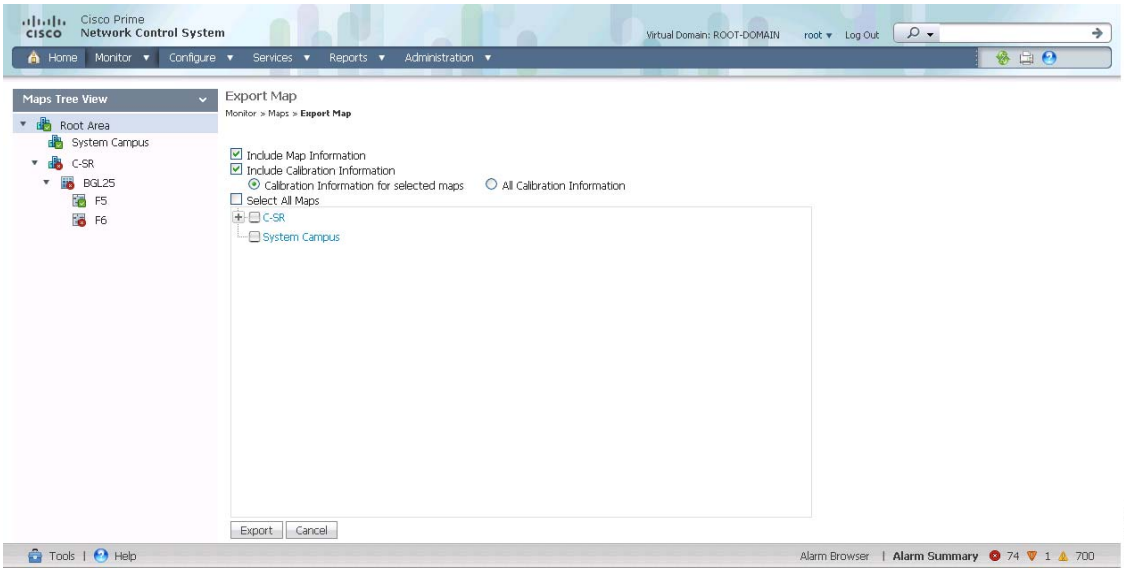
The Export Map feature allows you to export map or calibration information to XML. The exported XML is in an encrypted format and is readable. XML and images are bundled, tarred, and zipped into a file for a successful import into another NCS.

To export a map, follow these steps:

Step 1 Choose **Monitor > Site Maps** page.

Step 2 From the Select a command drop-down list, choose **Export Maps**. The Export Map page appears. (see Figure 4-9).

Figure 4-9 Export Map



Step 3 Select the maps that you want to export.

Step 4 Click **Export** to export the selected map data.

Importing a Map

The Import Map feature allows you to import map information from external sources such as XML, WLSE, and CSV. During import, the XML might be encrypted (if exported from the NCS) or unencrypted.

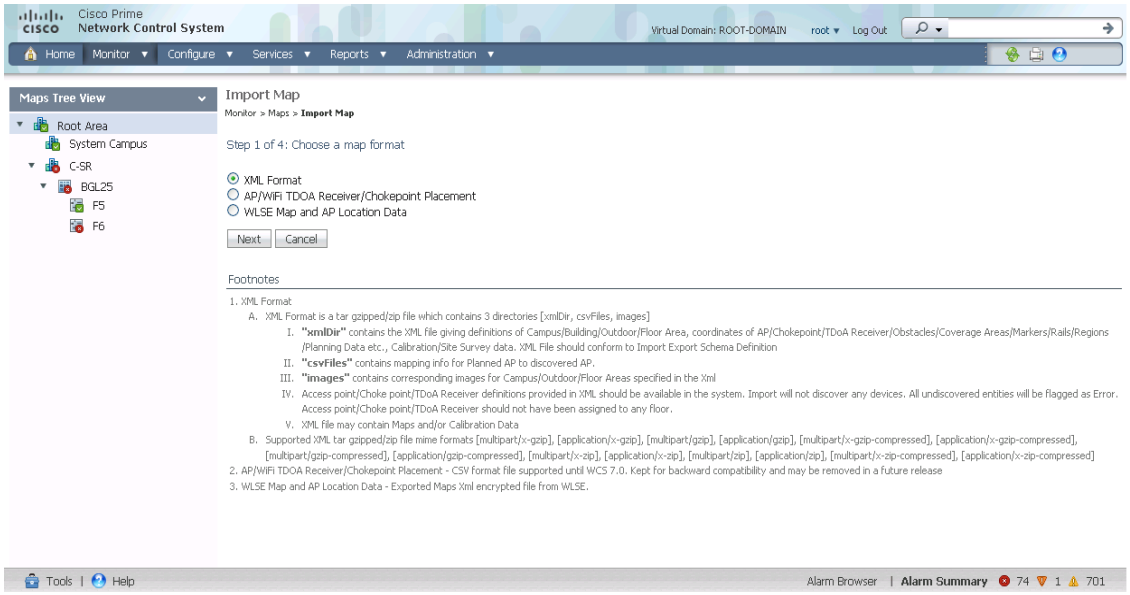
To import a map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 From the Select a command drop-down list, choose **Import Maps**. The Import Map page appears.

Note It is important that APs are first added to the NCS Server prior to importing maps, because APs in the maps are also included during the export process. APs that have not been added to the NCS server but are present in exported floor maps result in an error being displayed during importing these maps into the NCS. If APs are unassociated or unreachable, it results in the same error and you must manually add these APs to your maps after the importing process.

Figure 4-10 Import Map



Step 3 Choose the map format.

Step 4 Select one of the following formats:

- XML
- AP/WiFi TDOA Receiver/Chokepoint Placement
- WLSE Map and AP Location Data

Note The XML format option is available only to the root user.

Note The Aeroscout engine fails to start MSE if the NCS map names have special characters such as '&'.

Step 5 Click **Next**.

Step 6 Click **Browse** to select the file that you want to import.

Step 7 Click **Import** to import the selected data.

Editing Map Properties

To edit your map properties, follow these steps:

Note Users with Map read-write permissions can only edit the map properties.

Step 1 Choose **Monitor > Site Maps**.

Step 2 From the Select a command drop-down list, choose **Properties**.

Step 3 Click **Go**.

Step 4 Edit the information in Table 4-1.

Table 4-1 Map Properties Fields

Field or Control	Description
Unit of Dimension	Set dimension measurement in feet or meters for all NCS maps.
Wall Usage Calibration	Choose to use or not use walls, or set to automatic.
Refresh Map From Network	Enable refresh of map data for the NCS to update maps by polling the Cisco WLAN Solution each time a Cisco WLAN Solution operator requests a map update. Select the **Disable** check box to disable map updates for the NCS from its stored database. **Note** Updates to the database might not be frequent enough to keep the map data current.
Advanced Debug Mode	This option must be enabled on both the location appliance and the NCS to allow use of the location accuracy testpoint feature.
Use Dynamic Heatmaps	This option must be enabled to allow use of dynamic heatmaps. By default, it is enabled.
Minimum Number of APs for Dynamic Heatmaps	Dynamic heatmap of an AP is calculated only if it receives the RSSI strengths from a number of neighboring APs, which should be greater than or equal to this parameter value. The minimum and default is 4 and the maximum number of APs is 10.
Recomputation Frequency (Hours)	Configure the time when you want the data to be polled and refreshed when you are not actively using the maps. You can always refresh the data and get the latest heatmaps when you are actively using the maps. The default is 6 hours. The minimum is 1 hour and the maximum is 24 hours. We recommend a minimum number of APs as 4 and 6 hours as recomputation frequency for maximum performance.

Filtering Maps

In the Monitor > Site Maps page, the list of maps can be filtered based on type and status. To filter your map list, follow these steps:

Step 1 Choose **Monitor** > **Site Maps**.

Step 2 Choose the map type from the Type drop-down list. Map types include **All**, **Campus**, **Building**, **Outdoor Area**, and **Floor Area**.

Step 3 To further sort the map list by status, choose the status type from the Status drop-down list. Status types include **All**, **Critical**, **Major**, and **Minor**.

Note Status indicates the most serious level of alarm on an access point located on this map or one of its children.

Step 4 When the filtering criteria is selected, click **Go**. The list displays maps which fit the filtering criteria.

Configuring Buildings

You can add buildings to the NCS database regardless of whether you have added campus maps to the database. This section describes how to add a building to a campus map or a standalone building (one that is not part of a campus) to the NCS database.

This section contains the following topics:

Adding a Building to a Campus Map

To add a building to a campus map in the NCS database, follow these steps:

Step 1 Choose **Monitor** > **Site Maps** to display the Maps page.

Step 2 Click the desired campus. The Site Maps > Campus Name page appears.

Step 3 From the Select a command drop-down list, choose **New Building**, and click **Go** (see Figure 4-11).

Figure 4-11 New Building

Step 4 In the Campus Name > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:

a. Enter the building name.

b. Enter the building contact name.

c. Enter the number of floors and basements.

d. Enter the horizontal position (distance from the corner of the building rectangle to the left edge of the campus map) and the vertical position (distance from the corner of the building rectangle to the top edge of the campus map) in feet.

Note To change the unit of measurement (feet or meters), choose **Monitor > Site Maps**, and choose **Properties** from the Select a command drop-down list.

e. Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.

Note The horizontal and vertical span should be larger than or the same size as any floors that you might add later.

Tip You can also use **Ctrl-click** to resize the bounding area in the upper-left corner of the campus map. As you change the size of the bounding area, the Horizontal Span and Vertical Span parameters of the building change to match your actions.

f. Click **Place** to put the building on the campus map. The NCS creates a building rectangle scaled to the size of the campus map.

g. Click the building rectangle and drag it to the desired position on the campus map.

Note After adding a new building, you can move it from one campus to another without having to recreate it.

h. Click **Save** to save this building and its campus location to the database. The NCS saves the building name in the building rectangle on the campus map.

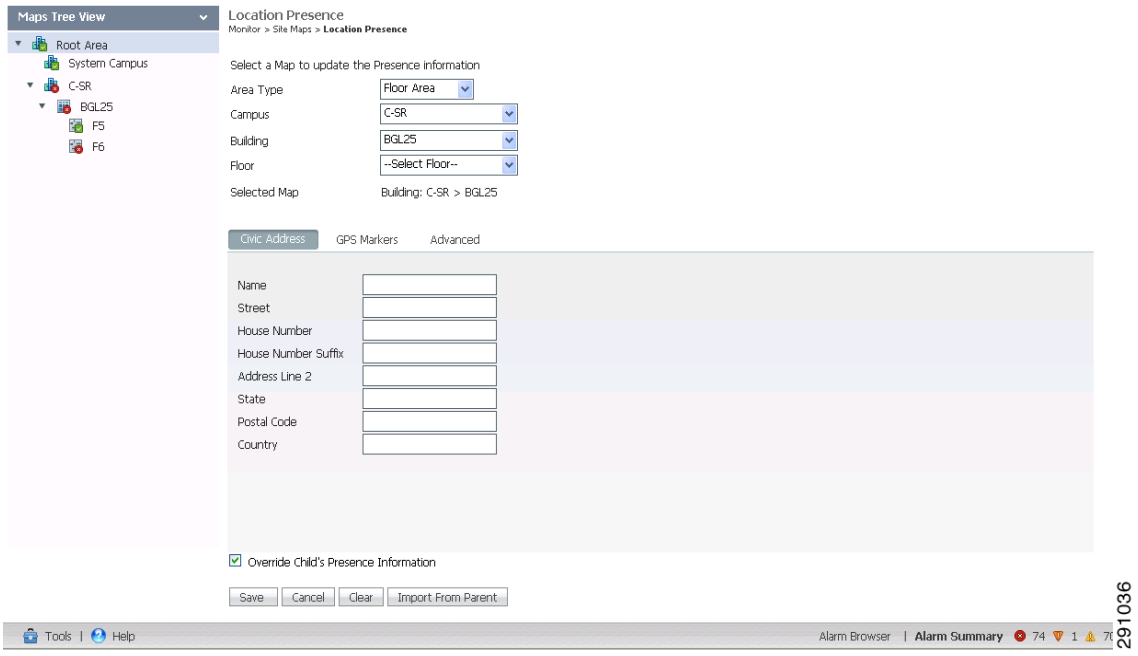
Note A hyperlink associated with the building takes you to the corresponding Map page.

Step 5 (Optional) To assign location presence information for the new outdoor area, do the following:

a. Choose **Edit Location Presence Info** from the Select a command drop-down list. Click **Go**. The Location Presence page appears (see Figure 4-12).

Note By default, the Presence Info check box of the Override Child Element is selected. This option should remain selected if you want to propagate the campus location to all buildings and floors on that campus. When adding buildings to the campus map, you can import the campus location information. The campus address cannot be imported to a building if the check box is unselected. This option should be unselected if you want to assign building-specific addresses to buildings on its campus rather than one campus address to all.

Figure 4-12 Location Presence



b. Click the **Civic Address**, **GPS Markers**, or **Advanced** tab.

- Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
- GPS Markers identify the campus by longitude and latitude.

– Advanced identifies the campus with expanded civic information such as neighborhood, city division, country, and postal community name.

Note Each selected field is inclusive of all of those above it. For example, if you choose Advanced, it can also provide GPS and Civic location information upon client demand. The selected setting must match what is set on the location server level (Services > Mobility Services).

Note If a client requests location information such as GPS Markers for a campus, building, floor, or outdoor area that is not configured for that field, an error message is returned.

c. By default, the Override Child's Presence Information check box is selected. There is no need to alter this setting for standalone buildings.

Step 6 Click **Save**.

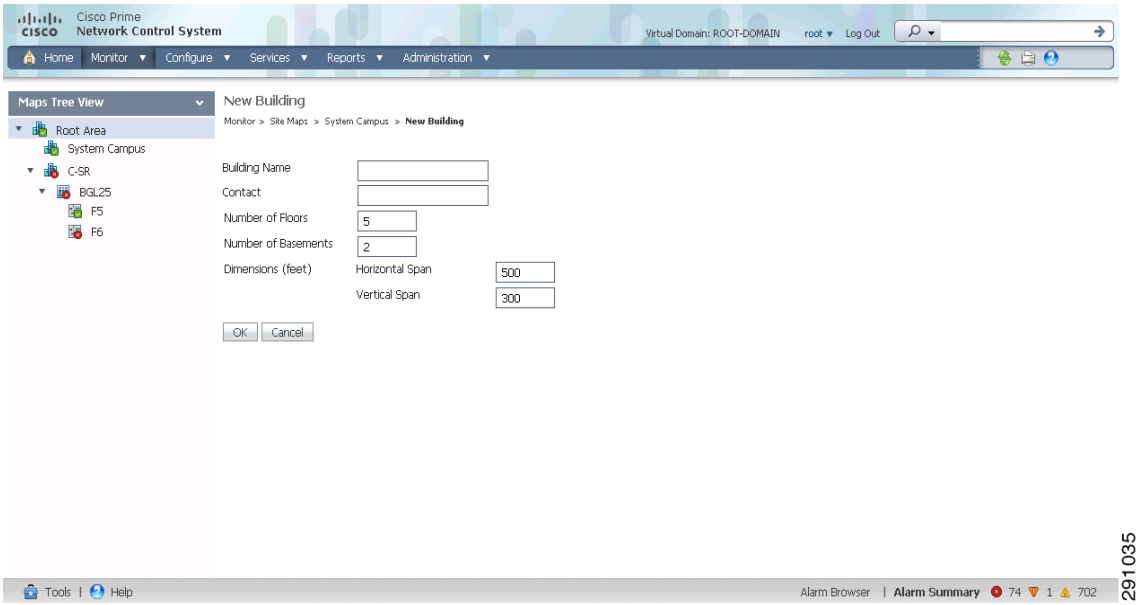
Adding a Standalone Building

To add a standalone building to the NCS database, follow these steps:

Step 1 Choose **Monitor > Site Maps** to display the Maps page.

Step 2 From the Select a command drop-down list, choose **New Building**, and click **Go** (see Figure 4-11).

Figure 4-13 New Standalone Building



Step 3 In the Maps > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:

a. Enter the building name.

b. Enter the building contact name.

Note After adding a new building, you can move it from one campus to another without having to recreate it.

c. Enter the number of floors and basements.

d. Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.

Note To change the unit of measurement (feet or meters), choose **Monitor > Site Maps**, and choose **Properties** from the Select a command drop-down list.

Note The horizontal and vertical span should be larger than or the same size as any floors that you might add later.

e. Click **OK** to save this building to the database.

Step 4 (Optional) To assign location presence information for the new building, do the following:

a. Choose **Location Presence** from the Select a command drop-down list. Click **Go**. The Location Presence page appears (see Figure 4-12).

b. Click the **Civic**, **GPS Markers**, or **Advanced** tab.

- Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
- GPS Markers identify the campus by longitude and latitude.
- Advanced identifies the campus with expanded civic information such as neighborhood, city division, county, and postal community name.

Note Each selected field is inclusive of all of those above it. For example, if you select Advanced, it can also provide GPS and Civic location information upon client demand. The selected setting must match what is set on the location server level (Services > Mobility Services).

Note If a client requests location information such as GPS Markers for a campus, building, floor, or outdoor area that is not configured for that field, an error message is returned.

c. By default, the Presence Info check box of the Override Child Element is selected. This option should remain selected if you want to propagate the campus location to all buildings and floors on that campus. When adding buildings to the campus map, you can import the location information. The campus address cannot be imported to a building if the check box is unselected. This option should be deselected if you want to assign building-specific addresses to buildings on its campus rather than one campus address to all.

Step 5 Click **Save**.

Note The standalone buildings are automatically placed in System Campus.

Viewing a Building

To view a current building map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the name of the building map to open its details page. The Building View page provides a list of floor maps and map details for each floor.

Note From the Building View page, you can click the Floor column heading to sort the list ascending or descending by floor.

The map details include the following:

- Floor area
- Floor index—Indicates the floor level. A negative number indicates a basement floor level.
- Contact
- Status—Indicates the most serious level of alarm on an access point located on this map or one of its children.
- Number of total access points located on the map.
- Number of 802.11a/n and 802.11b/g/n radios located on the map.
- Number of out of service (OOS) radios.
- Number of clients—Click the number link to view the Monitor > Clients page. See the "Monitoring Clients and Users" section on page 9-10 for more information.

Step 3 The Select a command drop-down list provides the following options:

- New Floor Area—See the "Adding Floor Areas to a Campus Building" section on page 4-28 or the "Adding Floor Plans to a Standalone Building" section on page 4-32 for more information.
- Edit Building—See the "Editing a Building" section on page 4-21 for more information.
- Delete Building—See the "Deleting a Building" section on page 4-22 for more information.
- Copy Building—See the "Copying a Map" section on page 4-11 for more information.
- Edit Location Presence Info—See the "Managing Location Presence Information" section on page 4-70 for more information.

Editing a Building

To edit a current building map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the name of the building map to open its details page.

Step 3 From the Select a command drop-down list, choose **Edit Building**.

Step 4 Make any necessary changes to Building Name, Contact, Number of Floors, Number of Basements, and Dimensions (feet).

Note To change the unit of measurement (feet or meters), choose **Monitor > Site Maps**, and choose **Properties** from the Select a command drop-down list.

Step 5 Click **OK**.

Deleting a Building

To delete a current building map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Select the check box for the building that you want to delete.

Step 3 Click **Delete** at the bottom of the map list (or choose **Delete Maps** from the Select a command drop-down list, and click **Go**).

Step 4 Click **OK** to confirm the deletion.

Note Deleting a building also deletes all of its container maps. The access points from all deleted maps are moved to an Unassigned state.

Moving a Building

To move a building to a different campus, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Select the check box of the applicable building.

Step 3 From the Select a command drop-down list, choose **Move Buildings**.

Step 4 Click **Go**.

Step 5 Choose the Target Campus from the drop-down list.

Step 6 Select the buildings that you want to move. Unselect any buildings that remain in their current location.

Step 7 Click **OK**.

Configuring Campus

This section contains the following topics:

Adding a Campus Map

To add a single campus map to the NCS database, follow these steps:

Step 1 Save the map in .PNG, .JPG, .JPEG, or .GIF format.

Note The map can be of any size because the NCS automatically resizes the map to fit its working areas.

Step 2 Browse to and import the map from anywhere in your file system.

Step 3 Choose **Monitor > Site Maps** to display the Maps page (see Figure 4-14).

Figure 4-14 New Campus

Step 4 From the Select a command drop-down list, choose **New Campus**, and click **Go**.

Step 5 In the Maps > New Campus page, enter the campus name and campus contact name.

Step 6 Browse to and choose the image filename containing the map of the campus, and click **Open**.

Step 7 Select the **Maintain Aspect Ratio** check box to prevent length and width distortion when the NCS resizes the map.

Step 8 Enter the horizontal and vertical span of the map in feet.

Note To change the unit of measurement (feet or meters), choose **Monitor > Site Maps** and choose **Properties** from the Select a command drop-down list. The horizontal and vertical span should be larger than any building or floor plan to be added to the campus.

Step 9 Click **OK** to add this campus map to the NCS database. The NCS displays the Maps page, which lists maps in the database, map types, and campus status.

Step 10 (Optional) To assign location presence information, click the newly created campus link in the Monitor > Site Maps page. See the "Managing Location Presence Information" section on page 4-70 for more information.

Viewing a Campus Map

To view a current campus map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the name of the campus map to open its details page.

Step 3 The Select a command drop-down list provides the following options:

- New Building—See the "Adding a Building to a Campus Map" section on page 4-16 for more information.
- New Outdoor Area—See the "Adding an Outdoor Area" section on page 4-25 for more information.
- Edit Campus—See the "Editing a Campus Map" section on page 4-24 for more information.
- Delete Campus—See the "Deleting a Campus Map" section on page 4-25 for more information.
- Copy Campus—See the "Copying a Map" section on page 4-11 for more information.
- Edit Location Presence Information—See the "Managing Location Presence Information" section on page 4-70 for more information.

Note Use the Monitor > Site Maps > Campus View main navigation bar at the top of the campus image to enlarge or decrease the size of the map view and to hide or show the map grid (which displays the map size in feet or meters).

Editing a Campus Map

The edit feature allows you to make changes to a current campus map. You can change the campus name, contact person, image, and map dimensions.

To edit a current campus map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the name of the campus map to open its details page.

Step 3 From the Select a command drop-down list, choose **Edit Campus**.

Step 4 Make any necessary changes to Campus Name, Contact, or Image File.

Step 5 Click **Next**.

Step 6 Make any additional changes to Maintain Aspect Ratio or Dimensions (feet).

Note To change the unit of measurement (feet or meters), choose **Monitor > Site Maps**, and choose **Properties** from the Select a command drop-down list.

Step 7 Click **OK**.

Deleting a Campus Map

To delete a current campus map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Select the check box for the campus that you want to delete.

Step 3 Click **Delete** at the bottom of the map list or choose **Delete Maps** from the Select a command drop-down list, and click **Go**.

Step 4 Click **OK** to confirm the deletion.

Note Deleting a campus also deletes all of its container maps. The access points from all deleted maps are moved to an Unassigned state.

Configuring Outdoor Areas

This section contains the following topics:

Adding an Outdoor Area

Note You can add an outdoor area to a campus map in the NCS database regardless of whether you have added outdoor area maps to the database.

To add an outdoor area to a campus map, follow these steps:

Step 1 If you want to add a map of the outdoor area to the database, save the map in .PNG, .JPG, .JPEG, or .GIF format. Then browse to and import the map from anywhere in your file system.

Note You do not need a map to add an outdoor area. You can simply define the dimensions of the area to add it to the database. The map can be any size because the NCS automatically resizes the map to fit the workspace.

Step 2 Choose **Monitor > Site Maps**.

Step 3 Click the desired campus to display the Monitor > Site Maps > Campus View page.

Step 4 From the Select a command drop-down list, choose **New Outdoor Area.**

Step 5 Click **Go**. The Create New Area page appears.

Step 6 In the New Outdoor Area page, enter the following information:

- Name—The user-defined name of the new outdoor area.
- Contact—The user-defined contact name.
- Area Type (RF Model)—Cubes And Walled Offices, Drywall Office Only, Outdoor Open Space (default).
- AP Height (feet)—Enter the height of the access point.
- Image File—Name of the file containing the outdoor area map. Click **Browse** to find the file.

Step 7 Click **Next**.

Step 8 Enter the following information:

- Zoom—Use to zoom in or zoom out on the map that you are currently viewing.
- Maintain Image Aspect Ratio—Select this check box to maintain the aspect ratio (ratio of horizontal and vertical pixels) of the map image. Maintaining the aspect ratio prevents visual distortion of the map.
- Horizontal Position—Distance from the corner of the outdoor area rectangle to the left edge of the campus map, in feet or meters.
- Vertical Position—Distance from the corner of the outdoor area rectangle to the top edge of the campus map, in feet or meters.
- Horizontal Span—Horizontal measurement (left to right) of the outdoor area rectangle, in feet or meters.
- Vertical Span—Vertical measurement (up and down) of the outdoor area rectangle, in feet or meters.

Tip The horizontal and vertical spans should be larger than or the same size. Use **Ctrl-click** to resize the bounding area in the upper-left corner of the campus map. The horizontal and vertical span parameters change to match.

Note To change the unit of measurement (feet or meters), choose **Monitor > Site Maps**, and choose **Properties** from the Select a command drop-down list.

Step 9 Click **Place** to put the outdoor area on the campus map. The NCS creates an outdoor area rectangle scaled to the size of the campus map.

Step 10 Click and drag the outdoor area rectangle to the desired position on the campus map.

Step 11 Click **Save** to save this outdoor area and its campus location to the database.

Note A hyperlink associated with the outdoor area takes you to the corresponding Maps page.

Step 12 (Optional) To assign location presence information for the new outdoor area, choose **Edit Location Presence Info**, and click **Go**. See the "Managing Location Presence Information" section on page 4-70 for more information.

Note By default, the Override Child Element Presence Info check box is selected. There is no need to alter this setting for outdoor areas.

Editing Outdoor Areas

To edit a current outdoor area, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the desired outdoor area map from the Name column.

Step 3 From the Select a command drop-down list, choose **Edit Outdoor Area**.

Step 4 Click **Go**.

Step 5 In the Campus Name > Outdoor Area page, edit the following information:

- Name—The user-defined name of the new outdoor area.
- Contact—The user-defined contact name.
- New Image File—Click **Browse** to import a new image file, if necessary.
- Maintain Image Aspect Ratio—Select this check box to maintain the aspect ratio (ratio of horizontal and vertical pixels) of the map image. Maintaining the aspect ratio prevents visual distortion of the map.
- Horizontal Position—Distance from the corner of the outdoor area rectangle to the left edge of the campus map, in ft. or meters.
- Vertical Position—Distance from the corner of the outdoor area rectangle to the top edge of the campus map, in ft. or meters.
- Horizontal Span—Horizontal measurement (left to right) of the outdoor area rectangle, in ft. or meters.
- Vertical Span—Vertical measurement (up and down) of the outdoor area rectangle, in ft. or meters.

Step 6 Click **Place** to put the outdoor area on the campus map. The NCS creates an outdoor area rectangle scaled to the size of the campus map.

Step 7 Click and drag the outdoor area rectangle to the desired position on the campus map.

Step 8 Click **Save** to save this outdoor area and its campus location to the database.

Note A hyperlink associated with the outdoor area takes you to the corresponding Maps page.

Deleting Outdoor Areas

To delete a current outdoor area, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Select the check box for the outdoor area that you want to delete.

Step 3 Click **Delete** at the bottom of the map list (or choose **Delete Maps** from the Select a command drop-down list, and click **Go**).

Step 4 Click **OK** to confirm the deletion.

Configuring Floor Areas

This section describes how to add floor plans to either a campus building or a standalone building in the NCS database and contains the following topics:

Adding Floor Areas to a Campus Building

After you add a building to a campus map, you can add individual floor plan and basement maps to the building.

To add a floor area to a campus building, follow these steps:

Step 1 Save your floor plan maps in .PNG, .JPG, or .GIF format.

Note The maps can be any size because the NCS automatically resizes the maps to fit the workspace.

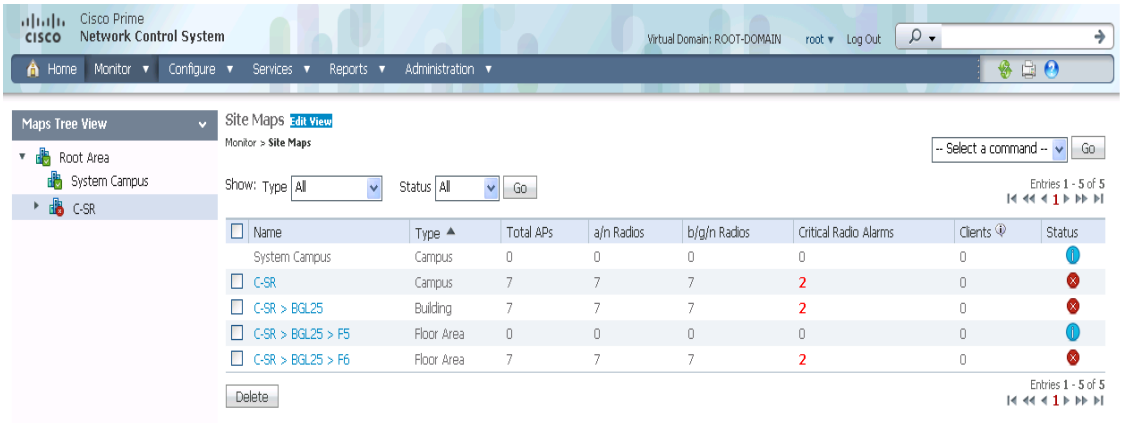
Step 2 Browse to and import the floor plan maps from anywhere in your file system. You can also import CAD image files DXF, and DWG.

Note If there are problems converting the auto-cad file, an error message is displayed. The NCS uses a native image conversion library to convert auto-cad files into raster formats like .PNG. If the native library cannot be loaded, the NCS displays an "unable to convert the auto-cad file" message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls NCS installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occur, you might need to install the required libraries and restart the NCS.

Note An imported auto-cad file can become blurred when you zoom. Without the zoom, the clarity is about the same as the original auto-cad file. Make sure all relevant sections are clearly visible in the original auto-cad file (DWG/DXF) and then import the auto-cad file into .PNG/.GIF format rather than .JPEG or .JPG.

Step 3 Choose **Monitor > Site Maps**. The Maps page appears (See Figure 4-15).

Figure 4-15 Monitor > Site Maps



Step 4 From the Maps Tree View or the Monitor > Site Maps list, choose the applicable campus building to open the Building View page.

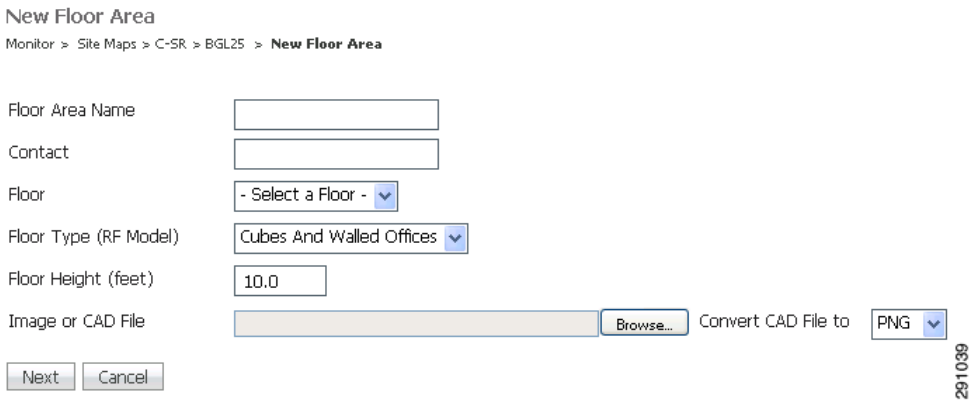
Step 5 Hover your mouse cursor over the name within an existing building rectangle to highlight it.

Note You can also access the building from the Campus View page. In the Campus View page, click the building name to open the Building View page.

Step 6 From the Select a command drop-down list, choose **New Floor Area**.

Step 7 Click **Go**. The New Floor Area page appears. (See Figure 4-16).

Figure 4-16 New Floor Area



Step 8 In the New Floor Area page, follow these steps to add floors to a building in which to organize related floor plan maps:

a. Enter the floor area and contact names.

b. Choose the floor or basement number from the Floor drop-down list.

c. Choose the floor or basement type (RF Model).

d. Enter the floor-to-floor height in feet.

Note To change the unit of measurement (feet or meters), choose **Monitor > Site Maps**, and choose **Properties** from the Select a command drop-down list.

e. Select the **Image or CAD File** check box.

f. Browse to and choose the desired floor or basement image or CAD filename, and click **Open**.

Note If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

Tip We do not recommend a .JPEG (.JPG) format for an auto-cad conversion. Unless a JPEG is specifically required, use .PNG or .GIF format for higher quality images.

g. Click **Next**. At this point, if a CAD file was specified, a default image preview is generated and loaded.

Note The NCS uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, the NCS displays the following error: "Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library." For more information see the NCS online help or NCS documentation.

The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

Note When you choose the floor or basement image filename, the NCS displays the image in the building-sized grid.

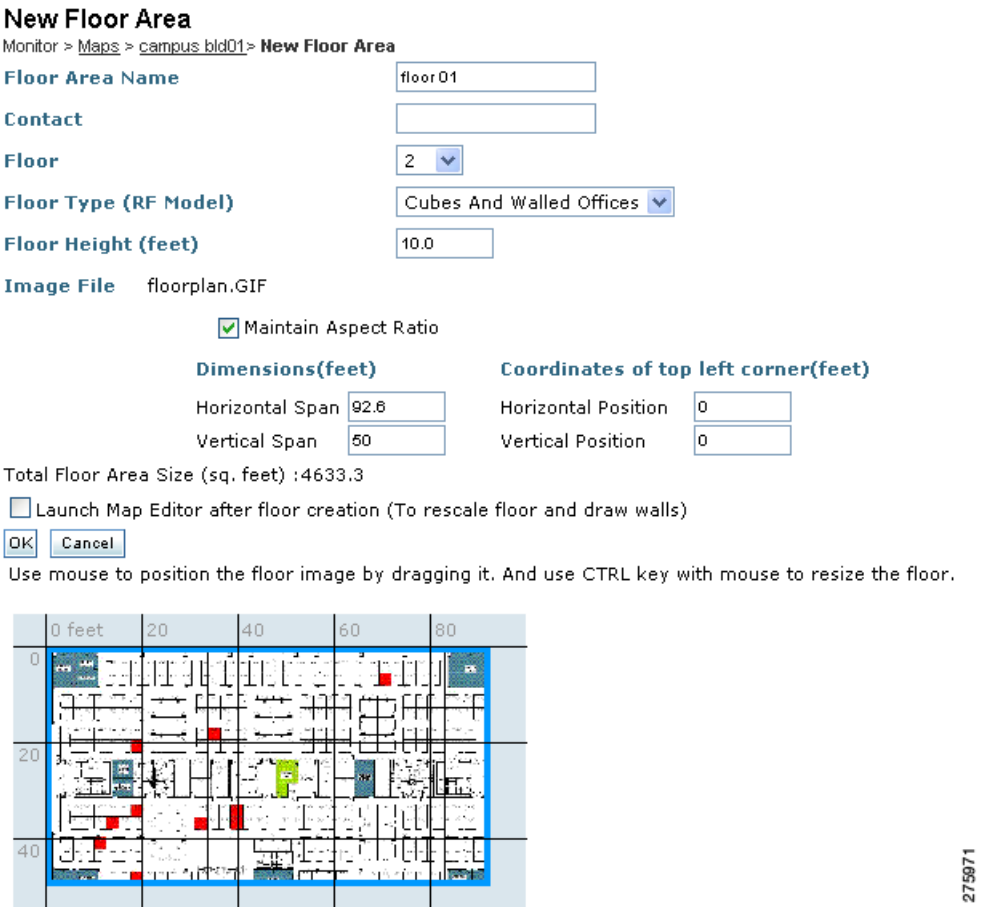
Note The maps can be any size because the NCS automatically resizes the maps to fit the workspace.

Note The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.

h. If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.

Enter the remaining parameters for the floor area (See Figure 4-17).

Figure 4-17 New Floor Area Fields



i. Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.

j. Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

Note The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the NCS database.

k. If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

Tip Use **Ctrl-click** to resize the image within the building-sized grid.

l. If desired, select the **Launch Map Editor after floor creation** check box to rescale the floor and draw walls.

m. Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Monitor > Site Maps list.

Note Use different floor names in each building. If you are adding more than one building to the campus map, do not use a floor name that exists in another building. This overlap causes incorrect mapping information between a floor and a building.

Step 9 Click any of the floor or basement images to view the floor plan or basement map.

Note You can zoom in or out to view the map at different sizes and you can add access points. See the "Adding Access Points to a Floor Area" section on page 4-34 for more information.

Adding Floor Plans to a Standalone Building

After you have added a standalone building to the NCS database, you can add individual floor plan maps to the building.

To add floor plans to a standalone building, follow these steps:

Step 1 Save your floor plan maps in .PNG, .JPG, or .GIF format.

Note The maps can be any size because the NCS automatically resizes the maps to fit the workspace.

Step 2 Browse to and import the floor plan maps from anywhere in your file system. You can import CAD files in DXF or DWG formats or any of the formats you created in Step 1.

Note If there are problems converting the auto-cad file, an error message is displayed. The NCS uses a native image conversion library to convert auto-cad files into raster formats like .PNG. If the native library cannot be loaded, the NCS displays an "unable to convert the auto-cad file" message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls NCS installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occur, you might need to install the required libraries and restart the NCS.

Note An imported auto-cad file can become blurred when you zoom. Without the zoom, the clarity is about the same as the original auto-cad file. Make sure all relevant sections are clearly visible in the original auto-cad file (DWG/DXF) and then import the auto-cad file into .PNG/.GIF format rather than .JPEG or .JPG.

Step 3 Choose **Monitor > Site Maps**.

Step 4 From the Maps Tree View or the Monitor > Site Maps left sidebar menu, choose the desired building to display the Building View page.

Step 5 From the Select a command drop-down list, choose **New Floor Area**.

Step 6 Click **Go**.

Step 7 In the New Floor Area page, add the following information:

- Enter the floor area and contact names.
- Choose the floor or basement number from the Floor drop-down list.
- Choose the floor or basement type (RF Model).
- Enter the floor-to-floor height in feet.
- Select the **Image or CAD File** check box.
- Browse to and choose the desired floor or basement Image or CAD file, and click **Open**.

Note If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

Tip A .JPEG (.JPG) format is not recommended for an auto-cad conversion. Unless a .JPEG is specifically required, use a .PNG or .GIF format for higher quality images.

Step 8 Click **Next**. At this point, if a CAD file was specified, a default image preview is generated and loaded.

Note The NCS uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, the NCS displays the following error: "Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library. For more information, see the NCS online help or NCS documentation."

The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

Note When you choose the floor or basement image filename, the NCS displays the image in the building-sized grid.

Note The maps can be any size because the NCS automatically resizes the maps to fit the workspace.

Note The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.

If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.

Step 9 Enter the remaining parameters for the floor area.

- Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.
- Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

Note The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the NCS database.

- If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

Tip Use **Ctrl-click** to resize the image within the building-sized grid.

- Adjust the floor characteristics with the NCS map editor by selecting the check box next to Launch Map Editor. See the "Map Editor" section on page 4-4 for more information regarding the map editor feature.

Step 10 Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Monitor > Site Maps list.

Step 11 Click any of the floor or basement images to view the floor plan or basement map.

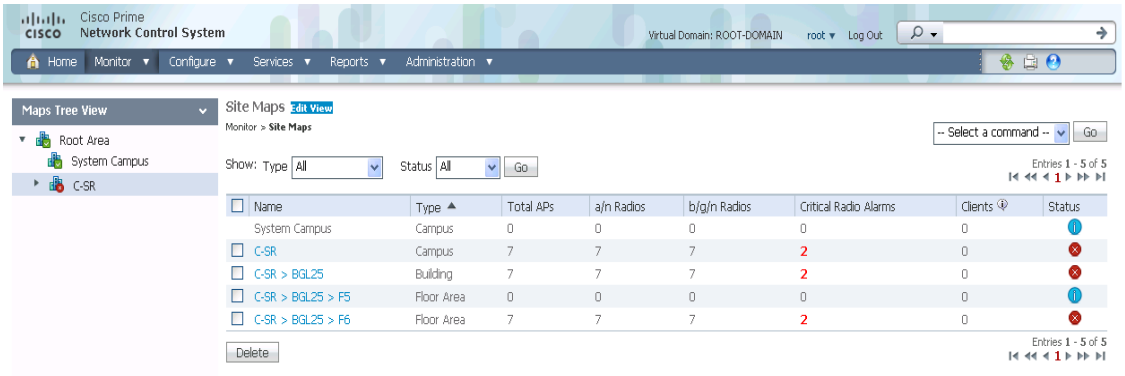
Note You can zoom in or out to view the map at different sizes and you can add access points. See the "Adding Access Points to a Floor Area" section on page 4-34 for more information.

Adding Access Points to a Floor Area

After you add the .PNG, .JPG, .JPEG, or .GIF format floor plan and outdoor area maps to the NCS database, you can position lightweight access point icons on the maps to show where they are installed in the buildings. To add access points to a floor area and outdoor area, follow these steps:

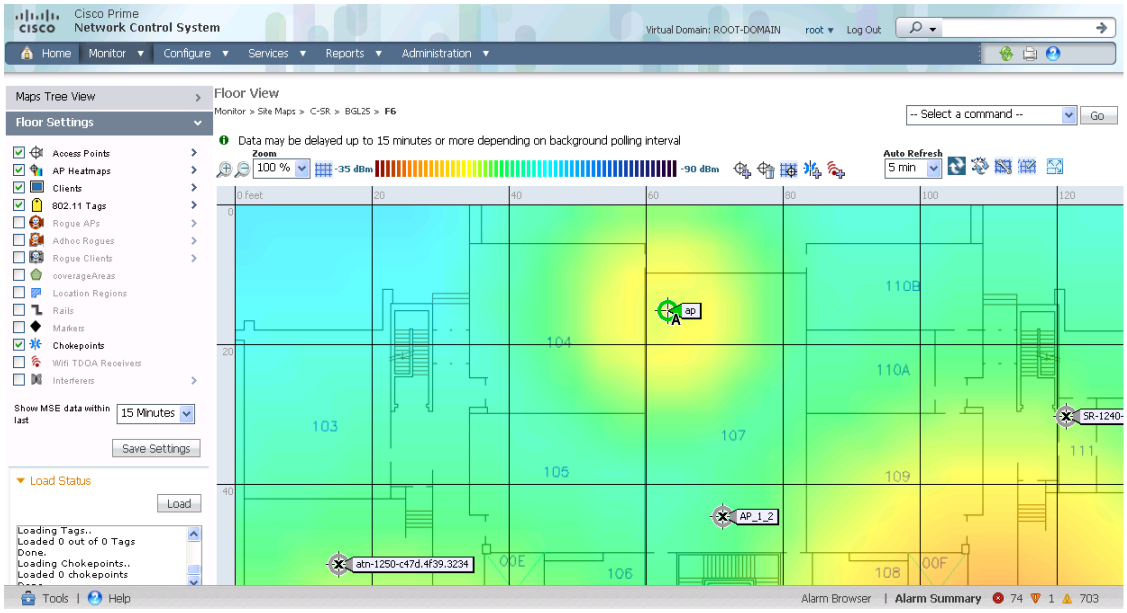
Step 1 Choose **Monitor > Site Maps**. The Maps page appears. (See Figure 4-18).

Figure 4-18 Monitor Site Maps



Step 2 From the Maps Tree View or the Monitor > Site Maps left sidebar menu, select the applicable floor to open the Floor View page. (See Figure 4-19).

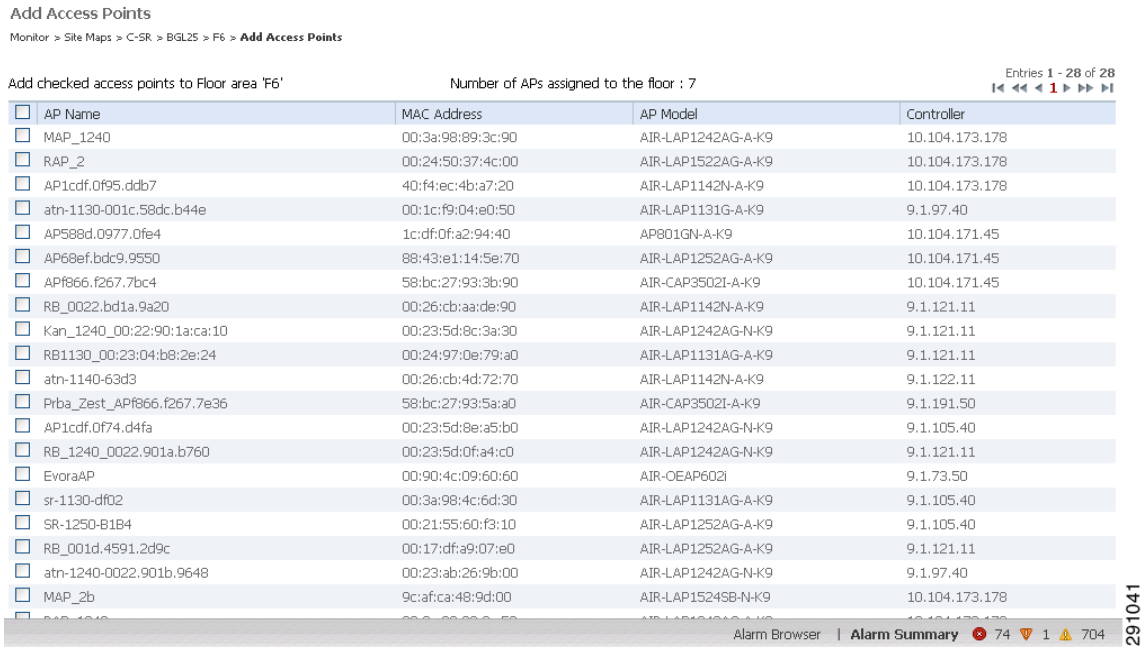
Figure 4-19 Floor View



Step 3 From the Select a command drop-down list, choose **Add Access Points,** and click **Go**.

Step 4 In the Add Access Points page, select the check boxes of the access points that you want to add to the floor area. (See Figure 4-20).

Figure 4-20 Add Access Point



Note Only access points that are not yet assigned to any floor or outdoor area appear in the list.

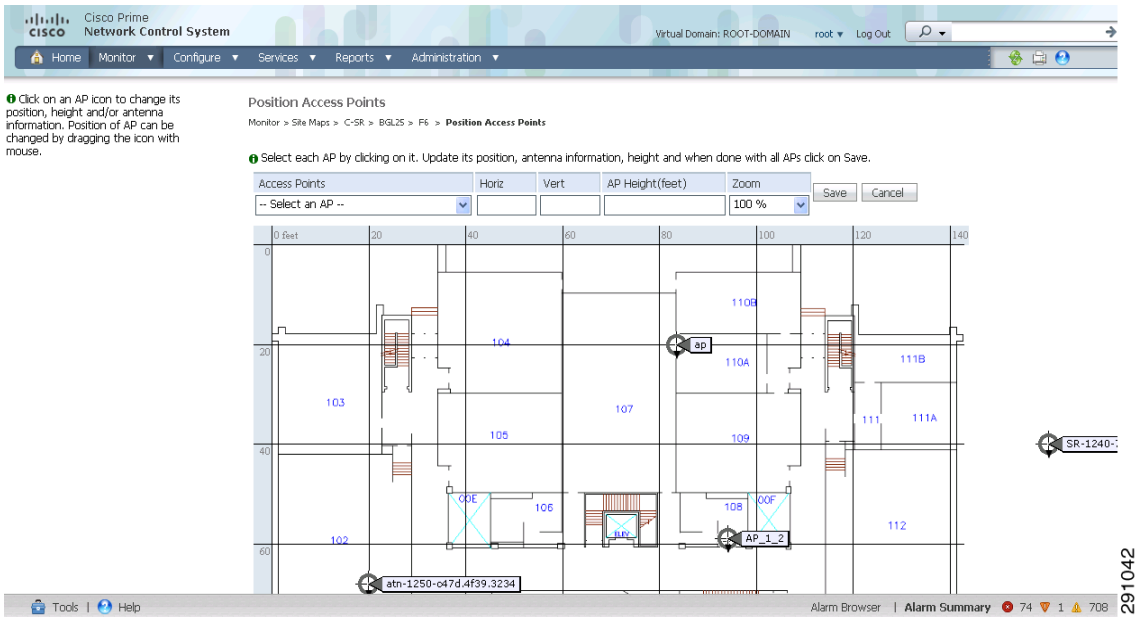
Note Select the check box at the top of the list to select all access points.

Note The NCS allows a maximum of 100 access points per floor map.

Step 5 When all of the applicable access points are selected, click **OK** located at the bottom of the access point list.

The Position Access Points page appears. (See Figure 4-21).

Figure 4-21 Position Access Points



Each access point you have chosen to add to the floor map is represented by a gray circle (differentiated by access point name or MAC address) and is lined up in the upper left part of the floor map.

Step 6 Click and drag each access point to the appropriate location. Access points turn blue when selected.

Note When you drag an access point on the map, its horizontal and vertical position appears in the Horiz and Vert text boxes.

Note The small black arrow at the side of each access point represents Side A of each access point, and each access point arrow must correspond with the direction in which the access points were installed. Side A is clearly noted on each 1000 series access point and has no relevance to the 802.11a/n radio. To adjust the directional arrow, choose the appropriate orientation from the Antenna Angle drop-down list.

When selected, the access point details are displayed on the left side of the page. Access point details include the following:

- AP Model—Indicates the model type of the selected access point.
- Protocol—Choose the protocol for this access point from the drop-down list.
- Antenna—Choose the appropriate antenna type for this access point from the drop-down list.
- Antenna/AP Image—The antenna image reflects the antenna selected from the Antenna drop-down list. Click the arrow at the top right of the antenna image to expand the image size.
- Antenna Orientation—Depending on the antenna type, enter the Azimuth and the Elevation orientations in degrees.

Note The Azimuth option does not appear for Omnidirectional antennas because their pattern is nondirectional in azimuth.

Note For internal antennas, the same elevation angle applies to both radios.

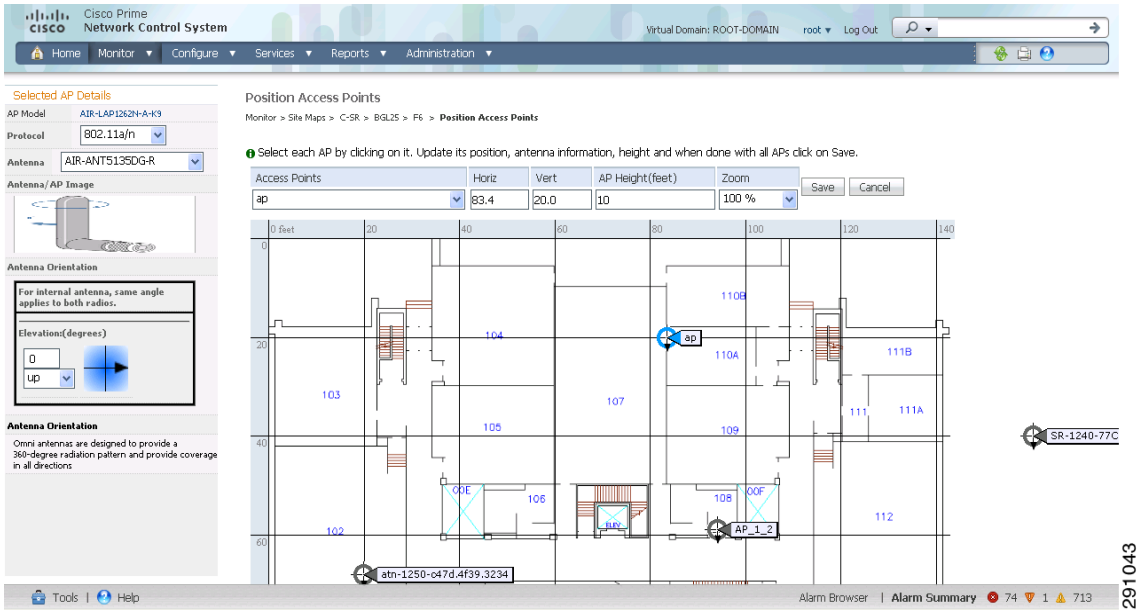
The antenna angle is relative to the map X axis. Because the origin of the X (horizontal) and Y (vertical) axes is in the upper left corner of the map, 0 degrees points side A of the access point to the right, 90 degrees points side A down, 180 degrees points side A to the left, and so on.

The antenna elevation is used to move the antenna vertically, up or down, to a maximum of 90 degrees.

Note Make sure each access point is in the correct location on the map and has the correct antenna orientation. Accurate access point positioning is critical when you use the maps to find coverage holes and rogue access points.

See the following URL for further information about the antenna elevation and azimuth patterns: http://www.cisco.com/en/US/products/hw/wireless/ps469/tsd_products_support_series_home.html

Figure 4-22 Selected Access Point Details



Step 7 When you are finished placing and adjusting each access point, click **Save**. (See Figure 4-22).

Note Clicking Save causes the antenna gain on the access point to correspond to the selected antenna. This might cause the radio to reset.

The NCS computes the RF prediction for the coverage area. These RF predictions are popularly known as *heat maps* because they show the relative intensity of the RF signals on the coverage area map.

Note This display is only an approximation of the actual RF signal intensity because it does not take into account the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions.

Note Antenna gain settings have no effect on heatmaps and location calculations. Antenna gain is implicitly associated to the antenna name. Because of this, the following apply:
– If an antenna is used and marked as “Other” in the NCS, it is ignored for all heatmap and location calculations;
– If an antenna is used and marked as a Cisco antenna in the NCS, that antenna gain setting (internal value on the NCS) is used no matter what gain is set on the controller.

Figure 4-23 RF Prediction Heatmaps

Note See the “Placing Access Points” section on page 4-40 for more information on placing access points on a map.

Note You can change the position of access points by importing or exporting a file. See the “Positioning Access Points, Wi-Fi TDOA Receivers, and Chokepoints by Importing or Exporting a File” section on page 4-56 for more information.

Removing Access Points

To remove access points, follow these steps:

Step 1 Choose **NCS > Monitor > Site Maps > System Campus > *Building* > *Floor***

The Floor View page appears.

Step 2 From the drop-down list towards the right, choose **Remove Access Points**, and click **Go**.

The Remove Access Points page appears.

Step 3 Select the check box next to the access points, which you want to delete and click **OK** to delete the selected access points.

Editing Floor Areas

To edit a current floor area, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the name of the floor area to open its details page.

Step 3 From the Select a command drop-down list, choose **Edit Floor Area**.

Step 4 Make any necessary changes to Floor Area Name, Contact, Floor, Floor Height (feet), Floor Type (RF Model), Existing Image File, or Import New Image File.

Step 5 Click **OK**.

Deleting Floor Areas

To delete a current floor area, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Select the check box for the applicable floor area.

Step 3 From the Select a command drop-down list, choose **Delete Maps**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Placing Access Points

To determine the best location of all devices in the wireless LAN coverage areas, you need to consider the access point density and location.

Ensure that no fewer than 3 access points, and preferably 4 or 5, provide coverage to every area where device location is required. The more access points that detect a device, the better. This high level guideline translates into the following best practices, ordered by priority:

1. Most importantly, access points should surround the desired location.
2. One access point should be placed roughly every 50 to 70 linear feet (about 17 to 20 meters). This translates into one access point every 2,500 to 5000 square feet (about 230 to 450 square meters).

Note The access point must be mounted so that it is under 20 feet high. For best performance, a mounting at 10 feet would be ideal.

Following these guidelines makes it more likely that access points detect tracked devices. Rarely do two physical environments have the same RF characteristics. Users might need to adjust these parameters to their specific environment and requirements.

Note Devices must be detected at signals greater than –75 dBm for the controllers to forward information to the location appliance. No fewer than three access points should be able to detect any device at signals below –75 dBm.

Note If you have a ceiling-mounted AP with an integrated omni-directional antenna, the antenna orientation does not really need to be set in the NCS. However, if you mount that same AP on the wall, you must set the antenna orientation to 90 degrees.

Table 4-2 describes the orientation of the access points.

Table 4-2 Antenna Orientation of the Access Points

Access Point	Antenna Orientation
1140 mounted on the ceiling	The Cisco logo should be pointing to the floor. Elevation: 0 degrees.
1240 mounted on the ceiling	The antenna should be perpendicular to the access point. Elevation: 0 degrees.
1240 mounted on the wall	The antenna should be parallel to the access point. Elevation: 0 degrees. If the antenna is perpendicular to the AP then the angle is 90 degrees (up or down does not matter as the dipole is omni).

Configuring Floor Settings

You can modify the appearance of the floor map by selecting or unselecting various floor settings check boxes. The selected floor settings appears in the map image.

Note Depending on whether or not a mobility services engine is present in the NCS, some of the floor settings might not be displayed. Clients, 802.11 Tags, Rogue APs, Adhoc Rogues, Rouge Clients, and Interferers are visible only if an MSE is present in the NCS.

The Floor Settings options include the following:

- Access Points—See the "Filtering Access Point Floor Settings" section on page 4-48 for more information.
- AP Heatmaps—See the "Filtering Access Point Heatmap Floor Settings" section on page 4-50 for more information.

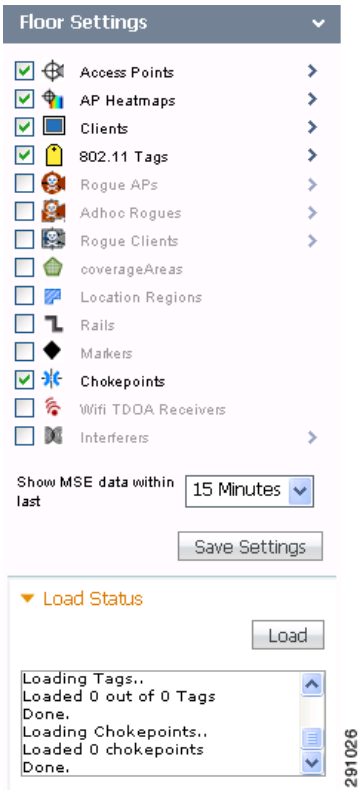
- AP Mesh Info—See the "Filtering AP Mesh Info Floor Settings" section on page 4-51 for more information.
- Clients—See the "Filtering Client Floor Settings" section on page 4-51 for more information.
- 802.11 Tags—See the "Filtering 802.11 Tag Floor Settings" section on page 4-53 for more information.
- Rogue APs—See the "Filtering Rogue AP Floor Settings" section on page 4-53 for more information.
- Rogue Adhocs—See the "Filtering Rogue Adhoc Floor Settings" section on page 4-54 for more information.
- Rogue Clients—See the "Filtering Rogue Client Floor Settings" section on page 4-54 for more information.
- Coverage Areas
- Location Regions
- Rails
- Markers
- Chokepoints
- Wi-Fi TDOA Receivers
- Interferers—See the "Filtering Interferer Settings" section on page 4-55 for more information.

Use the blue arrows to access floor setting filters for access points, access point heatmaps, clients, 802.11 tags, rogue access points, rogue adhocs, and rogue clients. When filtering options are selected, click **OK**.

Use the Show MSE data within last drop-down list to choose the timeframe for mobility services engine data. Choose to view mobility services engine data from a range including the past two minutes up to the past 24 hours. This option only appears if a mobility services engine is present on the NCS.

Click **Save Settings** to make the current view and filter settings your new default for all maps. (See Figure 4-24).

Figure 4-24 Floor Settings Fields



Defining Inclusion and Exclusion Regions on a Floor

To further refine location calculations on a floor, you can define the areas that are included (inclusion areas) in the calculations and those areas that are not included (exclusion areas).

For example, you might want to exclude areas such as an atrium or stairwell within a building but include a work area (such as cubicles, labs, or manufacturing floors).

Note If the MSE to which the floor is synchronized is running the Aeroscout tag engine, then inclusion and exclusion regions are not calculated for tags.

Viewing Floor Component Details

To view details regarding the components displayed on the Floor View, hover your mouse cursor over the applicable icon. A dialog box containing detailed information is displayed. Table 4-3 displays the floor map icons.

Table 4-3 Floor Map Icons

Icon	Description
	Access point icon. The color of the circle indicates the alarm status of the Cisco Radios. **Note** Each access point contains two Cisco Radios. When a single protocol is selected in the Access Point filter page, the entire icon represents this radio. If both protocols are selected, the top half of the icon represents the state of the 802.11a/n radio and the bottom half represents the state of the 802.11b/g/n radio. **Note** If a Cisco Radio is disabled, a small "x" appears in the middle of the icon. **Note** Monitor mode access points are shown with a gray label to distinguish these from other access points.
	AP heatmaps icon.
	Client icon. Hover your mouse cursor over the icon to view client details. See the "Client Details" section on page 4-106 for more information.
	Tag icon. Hover your mouse cursor over the icon to view tag details. See the "Tag Details" section on page 4-107 for more information.
	Rogue access point icon. The color of the icon indicates the type of rogue access point. For example, red indicates a malicious rogue access point and blue indicates an unknown type. Hover your mouse cursor over the icon to view rogue access point details. See the "Rogue Access Point Details" section on page 4-107 for more information.
	Rogue adhoc icon. Hover your mouse cursor over the icon to view rogue adhoc details. See the "Rogue Adhoc Details" section on page 4-108 for more information.
	Rogue client icon. Hover your mouse cursor over the icon to view rogue client details. See the "Rogue Client Details" section on page 4-108 for more information.
	Coverage icon.
	Location regions icon.
	Rails icon.

Table 4-3 Floor Map Icons (continued)

Icon	Description
	Marker icon.
	Chokepoint icon. See the "Chokepoints" section on page 4-4 for more information.
	Wi-Fi TDOA receiver icon. See the "Adding Wi-Fi TDOA Receivers to a Map" section on page 4-62 for more information.
	Interferer device icon. See the "Interferer Details" section on page 4-108 for more information.

Cisco 1000 Series Lightweight Access Point Icons

The icons indicate the present status of an access point. The circular part of the icon can be split in half horizontally. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.

Note When the icon is representing 802.11a/n and 802.11b/n, the top half displays the 802.11a/n status, and the bottom half displays the 802.11b/g/n status. When the icon is representing only 802.11b/g/n, the whole icon displays the 802.11b/g/n status. The triangle indicates the more severe color.

Table 4-4 shows the icons used in the NCS user interface Map displays.

Table 4-4 Access Points Icons Description

Icon	Description
	The green icon indicates an access point (AP) with no faults. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio.
	The yellow icon indicates an access point with a minor fault. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio. **Note** A flashing yellow icon indicates that there has been an 802.11a or 802.11b/g interference, noise, coverage, or load Profile Failure. A flashing yellow icon indicates that there have been 802.11a and 802.11b/g profile failures.
	The red icon indicates an access point (AP) with a major or critical fault. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio.
	The dimmed icon with a question mark in the middle represents an unreachable access point. It is gray because its status cannot be determined.

Table 4-4 Access Points Icons Description (continued)

Icon	Description
	The dimmed icon with no question mark in the middle represents an unassociated access point.
	The icon with a red “x” in the center of the circle represents an access point that has been administratively disabled.
	The icon with the top half green and the lower half yellow indicates that the optional 802.11a Cisco Radio (top) has no faults, and the 802.11b/g Cisco Radio (bottom) has a minor fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half green and the lower half red indicates that the optional 802.11a Cisco Radio (top) is operational with no faults, and the 802.11b/g Cisco Radio (bottom) has a major or critical fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half yellow and the lower half red indicates that the optional 802.11a Cisco Radio (top) has a minor fault, and the 802.11b/g Cisco Radio (bottom) has a major or critical fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half yellow and the lower half green indicates that the optional 802.11a Cisco Radio (top) has a minor fault, and the 802.11b/g Cisco Radio (bottom) is operational with no faults. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half red and the lower half green indicates that the optional 802.11a Cisco Radio (top) has a major or critical fault, and the 802.11b/g Cisco Radio (bottom) is operational with no faults. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.

Table 4-4 Access Points Icons Description (continued)

Icon	Description
	The icon with the top half red and the lower half yellow indicates that the optional 802.11a Cisco Radio (top) has major or critical faults, and the 802.11b/g Cisco Radio (bottom) has a minor fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
     	The icon with a red “x” on the top half (optional 802.11a) shows that the indicated Cisco Radio has been administratively disabled. There are six color coding possibilities as shown.

Each of the access point icons includes a small black arrow that indicates the direction in which the internal Side A antenna points.

Table 4-5 shows some arrow examples used in the NCS user interface map displays.

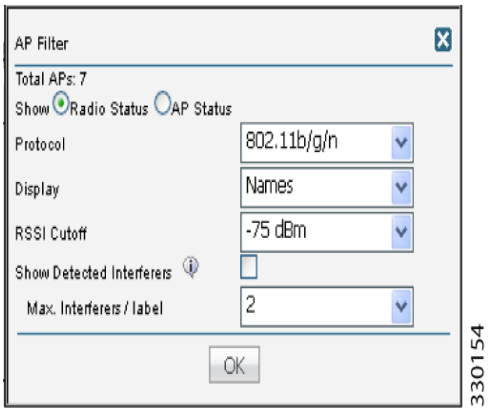
Table 4-5 Arrows

Arrow Examples	Direction
	Zero degrees, or to the right on the map.
	45 degrees, or to the lower right on the map.
	90 degrees, or down on the map.
These examples show the first three 45-degree increments allowed, with an additional five at 45-degree increments.	

Filtering Access Point Floor Settings

If you enable the access point floor setting and then click the blue arrow to the right of the floor settings, the Access Point Filter dialog box appears with filtering options. (See Figure 4-25).

Figure 4-25 Access Point Filter



Access point filtering options include the following:

- Show—Select this radio button to display the radio status or the access point status.

  Note Because the access point icon color is based on the access point status, the icon color might vary depending on the status selected. The default on floor maps is radio status.

- Protocol—From the drop-down list, choose which radio types to display (802.11a/n, 802.11b/g/n, or both).

  Note The displayed heatmaps correspond to the selected radio type(s).

- Display—From the drop-down list, choose what identifying information is displayed for the access points on the map image.
  - Channels—Displays the Cisco Radio channel number or Unavailable (if the access point is not connected).

    Note The available channels are defined by the country code setting and are regulated by country. See the following URL for more information: http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html

  - TX Power Level—Displays the current Cisco Radio transmit power level (with 1 being high) or Unavailable (if the access point is not connected).

    Note The power levels differ depending on the type of access point. The 1000 series access points accept a value between 1 and 5, the 1230 access points accept a value between 1 and 7, and the 1240 and 1100 series access points accept a value between 1 and 8.

Table 4-6 lists the transmit power level numbers and their corresponding power setting.

Table 4-6 Transmit Power Level Values

Transmit Power Level Number	Power Setting
1	Maximum power allowed per country code setting
2	50% power
3	25% power
4	12.5 to 6.25% power
5	6.25 to 0.195% power

Note The power levels are defined by the country code setting and are regulated by country. See the following URL for more information: http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html

- Channel and Tx Power—Displays both the channel and transmit power level (or Unavailable if the access point is not connected).
- Coverage Holes—Displays a percentage of clients whose signal has become weaker until the client lost its connection, Unavailable for unconnected access points, or MonitorOnly for access points in monitor-only mode.

Note Coverage holes are areas in which clients cannot receive a signal from the wireless network. When you deploy a wireless network, you must consider the cost of the initial network deployment and the percentage of coverage hole areas. A reasonable coverage hole criterion for launch is between 2 and 10 percent. This means that between two and ten test locations out of 100 random test locations might receive marginal service. After launch, Cisco Unified Wireless Network Solution Radio Resource Management (RRM) identifies these coverage hole areas and reports them to the IT manager, who can fill holes based on user demand.

- MAC Addresses—Displays the MAC address of the access point, whether or not the access point is associated to a controller.
- Names—Displays the access point name. This is the default value.
- Controller IP—Displays the IP address of the controller to which the access point is associated or Not Associated for disassociated access points.
- Utilization—Displays the percentage of bandwidth used by the associated client devices (including receiving, transmitting, and channel utilization). Displays Unavailable for disassociated access points and MonitorOnly for access points in monitor-only mode.
- Profiles—Displays the load, noise, interference, and coverage components of the corresponding operator-defined thresholds. Displays Okay for thresholds not exceeded, Issue for exceeded thresholds, or Unavailable for unconnected access points.

Note Use the Profile Type drop-down list to choose Load, Noise, Interference, or Coverage.

- CleanAir Status—Displays the CleanAir status of the access point and whether or not CleanAir is enabled on the access point.
- Average Air Quality—Displays the average air quality on this access point. The details include the band and the average air quality.
- Minimum Air Quality—Displays the minimum air quality on this access point. The details include the band and the minimum air quality.
- Average and Minimum Air Quality—Displays the average and minimum air quality on this access point. The details include the band, average air quality, and minimum air quality.
- Associated Clients—Displays the number of associated clients, Unavailable for unconnected access points or MonitorOnly for access points in monitor-only mode.

Note Click the client number to view client details. See "Monitoring Clients and Users" section on page 9-10 for more information.

- Bridge Group Names

- RSSI Cutoff—From the drop-down list, choose the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBm.
- Show Detected Interferers—Select the check box to display all interferers detected by the access point.
- Max. Interferers/label—Choose the maximum number of interferers to be displayed per label from the drop-down list.

Click **OK** when all applicable filtering criteria are selected.

Filtering Access Point Heatmap Floor Settings

An RF heatmap is a graphical representation of RF wireless data where the values taken by variables are represented in maps as colors. The current heatmap is computed based on the RSSI prediction model, Antenna Orientation, and AP transmit power.

If you enable the Access Point Heatmap floor setting and click the blue arrow to the right of the Floor Settings, the Contributing APs dialog appears with heatmap filtering options. See the "Understanding RF Heatmap Calculation" section on page 4-110 for more information.

The NCS introduces dynamic heatmaps. When dynamic heatmaps are enabled, the NCS recomputes the heatmaps to represent changed RSSI values. To configure the dynamic heatmaps, see the "Editing Map Properties" section on page 4-14 for more information.

Access point heatmap filtering options include the following:

- Heatmap Type—Select Coverage, or Air Quality. If you choose Air Quality, you can further filter the heat map type for access points with average air quality or minimum air quality. Select the appropriate radio button.

Note If you have monitor mode access points on the floor plan, you have a choice between IDS or coverage heatmap types. A coverage heatmap excludes monitor mode access points.

Note Only APs in Local, FlexConnect, or Bridge mode can contribute to the Coverage and Air Quality Heatmap.

- Total APs—Displays the number of access points positioned on the map.
- Select the access point check box(es) to determine which heatmaps are displayed on the image map.

Click **OK** when all applicable filtering criteria are selected.

Filtering AP Mesh Info Floor Settings

Note The AP Mesh Info check box only appears when bridging access points are added to the floor.

When this check box is selected, the NCS initiates a contact with the controllers and displays information about bridging access points. The following information is displayed:

- Link between the child and the parent access point.
- An arrow that indicates the direction from the child to parent access point.
- A color-coded link that indicates the signal-to-noise ratio (SNR). A green link represents a high SNR (above 25 dB), an amber link represents an acceptable SNR (20-25 dB), and a red link represents a very low SNR (below 20 dB).

If you enable the AP Mesh Info floor setting and click the blue arrow to the right of the floor settings, the Mesh Parent-Child Hierarchical View page appears with mesh filtering options.

You can update the map view by choosing the access points you want to see on the map. From the Quick Selections drop-down list, choose to select only root access point, various hops between the first and the fourth, or select all access points.

Note For a child access point to be visible, its parent must also be selected.

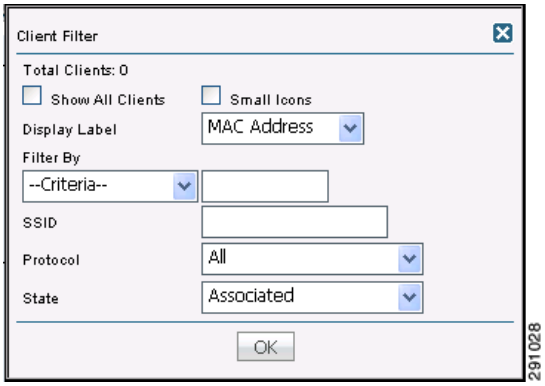
Click **OK** when all applicable filtering criteria are selected.

Filtering Client Floor Settings

Note The Clients option only appears if a mobility server is added in the NCS.

If you enable the Clients floor setting and click the blue arrow to the right, the Client Filter dialog box appears.

Figure 4-26 Client Filter



Client filtering options include the following:

- Show All Clients—Select the check box to display all clients on the map.
- Small Icons—Select the check box to display icons for each client on the map.

Note If you select the **Show All Clients** check box and **Small Icons** check box, all other drop-down list options are dimmed.

If you unselect the **Small Icons** check box, you can choose if you want the label to display the MAC address, IP address, username, asset name, asset group, or asset category.

If you unselect the **Show All Clients** check box, you can specify how you want the clients filtered and enter a particular SSID.

- Display—Choose the client identifier (IP address, username, MAC address, asset name, asset group, or asset category) to display on the map.
- Filter By—Choose the parameter by which you want to filter the clients (IP address, username, MAC address, asset name, asset group, asset category, or controller). Once selected, type the specific device in the text box.

Note Beginning with NCS Release 1.1 and later, you can not only filter IPv4 addresses but also IPv6 addresses as well. You can also specify partial IPv6 addresses as filter criteria.

Note If there are multiple IPv6 addresses for a client, then you can specify any one IP address to uniquely identify the client.

- SSID—Enter the client SSID in the available text box.
- Protocol—Choose All, 802.11a/n, or 802.11b/g/n from the drop-down list.
  - All—Displays all the access points in the area.
  - 802.11a/n—Displays a colored overlay depicting the coverage patterns for the clients with 802.11a/n radios. The colors show the received signal strength from red (–35 dBm) through dark blue (–85 dBm).

  - 802.11b/g/n—Displays a colored overlay depicting the coverage patterns for the clients with 802.11b/g/n radios. The colors show the received signal strength from red (–35 dBm) through dark blue (–85 dBm). This is the default value.

- State—Choose All, Idle, Authenticated, Probing, or Associated from the drop-down list.

Click **OK** when all applicable filtering criteria are selected.

Filtering 802.11 Tag Floor Settings

If you enable the 802.11 Tags floor setting and then click the blue arrow to the right, the Tag Filter dialog appears.

Tag filtering options include the following:

- Show All Tags—Select the check box to display all tags on the map.
- Small Icons—Select the check box to display icons for each tag on the map.

Note If you select the Show All Tags check box and Small Icons check box, all other drop-down list options are dimmed.

If you unselect the Small Icons check box, you can choose if you want the label to display MAC address, asset name, asset group, or asset category.

If you unselect the Show All Tags check box, you can specify how you want the tags filtered.

- Display—Choose the tag identifier (MAC address, asset name, asset group, or asset category) to display on the map.
- Filter By—Choose the parameter by which you want to filter the clients (MAC address, asset name, asset group, asset category, or controller). Once selected, type the specific device in the text box.

Click **OK** when all applicable filtering criteria are selected.

Filtering Rogue AP Floor Settings

If you enable the Rogue APs floor setting and then click the blue arrow to the right, the Rogue AP filter dialog box appears.

Rogue AP filtering options include the following:

- Show All Rogue APs—Select the check box to display all rogue access points on the map.
- Small Icons—Select the check box to display icons for each rogue access point on the map.

Note If you select the **Show All Rogue APs** check box and **Small Icons** check box, all other drop-down list options are dimmed.

If you unselect the **Show All Rogue APs** check box, you can specify how you want the rogue access points filtered.

- MAC Address—If you want to view a particular MAC address, enter it in the MAC Address text box.
- State—Use the drop-down list to choose from Alert, Known, Acknowledged, Contained, Threat, or Unknown contained states.

- On Network—Use the drop-down list to specify whether or not you want to display rogue access points on the network.

Click **OK** when all applicable filtering criteria are selected.

Filtering Rogue Adhoc Floor Settings

If you enable the Rogue Adhocs floor setting and then click the blue arrow to the right, the Rogue Adhoc filter dialog appears.

Rogue Adhoc filtering options include the following:

- Show All Rogue Adhocs—Select the check box to display all rogue adhoc on the map.
- Small Icons—Select the check box to display icons for each rogue adhoc on the map.

Note If you select the **Show All Rogue Adhocs** check box and **Small Icons** check box, all other drop-down list options are dimmed.

If you unselect the **Show All Rogue Adhocs** check box, you can specify how you want the rogue adhocs filtered.

- MAC Address—If you want to view a particular MAC address, enter it in the MAC Address text box.
- State—Use the drop-down list to select from Alert, Known, Acknowledged, Contained, Threat, or Unknown contained states.
- On Network—Use the drop-down list to specify whether or not you want to display rogue adhocs on the network.

Click **OK** when all applicable filtering criteria are selected.

Filtering Rogue Client Floor Settings

If you enable the Rogue Clients floor setting and then click the blue arrow to the right, the Rogue Clients filter dialog appears.

Rogue Clients filtering options include the following:

- Show All Rogue Clients—Select the check box to display all rogue clients on the map.
- Small Icons—Select the check box to display icons for each rogue client on the map.

Note If you select the **Show All Rogue Clients** check box and **Small Icons** check box, all other drop-down list options are dimmed. If you unselect the **Show All Rogue Clients** check box, you can specify how you want the rogue clients filtered.

- Assoc. Rogue AP MAC Address—If you want to view a particular MAC address, enter it in the MAC Address text box.
- State—Use the drop-down list to choose from Alert, Contained, Threat, or Unknown contained states.

Click **OK** when all applicable filtering criteria are selected.

Filtering Interferer Settings

If you enable Interferer floor setting and then click the blue arrow to the right, the Interferers filter dialog box appears.

Interferer filtering options include the following:

- Show active interferers only—Select the check box to display all active interferers.
- Small Icons—Select the check box to display icons for each interferer on the map.
- Show Zone of Impact—Displays the approximate interference impact area. The opacity of the circle denotes its severity. A solid red circle represents a very strong interferer that likely disrupts Wi-Fi communications, a light pink circle represents a weak interferer.
- Click **OK** when all applicable filtering criteria are selected.

Import Map and AP Location Data

When converting from autonomous to lightweight access points and from the WLSE to the NCS, one of the conversion steps is to manually reenter the access point-related information into the NCS. To speed up this process, you can export the information about access points from the WLSE and import it into the NCS.

Note The NCS expects a .tar file and checks for a .tar extension before importing the file. If the file you are trying to import is not a .tar file, the NCS displays an error message and prompts you to import a different file.

Note For more information on the WLSE data export functionality (WLSE Version 2.15), see the following URL:
http://<WLSE_IP_ADDRESS>:1741/debug/export/exportSite.jsp.

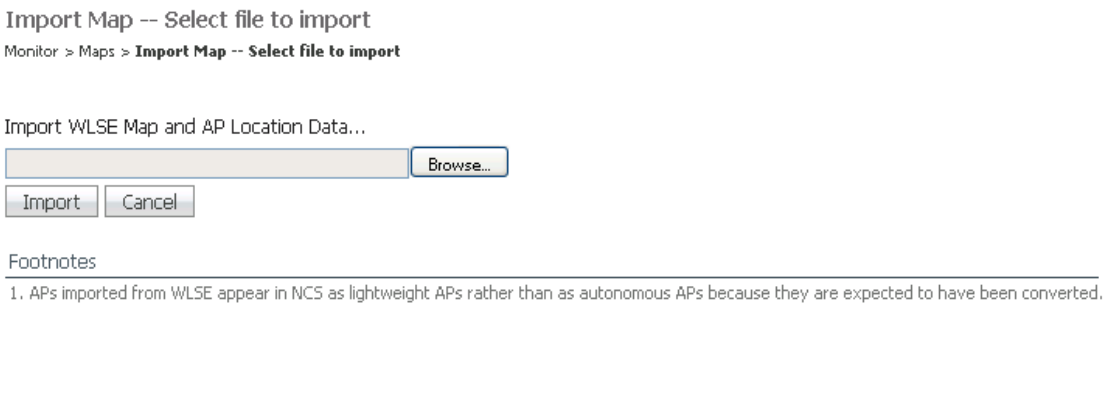
To map properties and import a tar file containing WLSE data using the NCS web interface, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 From the Select a command drop-down list, choose **Import Maps**, and click **Go**.

Step 3 Choose the **WLSE Map and AP Location Data** option, and click **Next**. (See Figure 4-27).

Figure 4-27 Import WLSE Map and AP Location Data



Step 4 In the Import WLSE Map and AP Location Data page, click **Browse** to select the file to import.

Step 5 Find and select the .tar file to import and click **Open**.

The NCS displays the name of the file in the Import From text box.

Step 6 Click **Import**.

The NCS uploads the file and temporarily saves it into a local directory while it is being processed. If the file contains data that cannot be processed, the NCS prompts you to correct the problem and retry. Once the file has been loaded, the NCS displays a report of what is added to the NCS. The report also specifies what cannot be added and why.

If some of the data to be imported already exists, the NCS either uses the existing data in the case of campuses or overwrites the existing data using the imported data in the cases of buildings and floors.

Note If there are duplicate names between a WLSE site and building combination and an NCS campus (or top-level building) and building combination, the NCS displays a message in the Pre Execute Import Report indicating that it will delete the existing building.

Step 7 Click **Import** to import the WLSE data.

The NCS displays a report indicating what was imported.

Step 8 Choose **Monitor > Site Maps** to view the imported data.

Positioning Access Points, Wi-Fi TDOA Receivers, and Chokepoints by Importing or Exporting a File

To change an access point, Wi-Fi TDOA receiver, or chokepoint position, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 From the Select a command drop-down list, choose **Properties**.

Step 3 From the Unit of Dimension drop-down list, choose **feet** or **meters**.

Step 4 Select the Advanced Debug Mode **Enable** radio button.

Step 5 Click **OK**.

Step 6 From the Select a command drop-down list, choose **Export/Import AP/WiFi TDOA Receiver/Chokepoint Placement**.

Step 7 In the Import/Export AP/WiFi TDOA Receiver/Chokepoint Placement page, click **Browse** to find the file you want to import.

Note The file must already be created and added to the NCS.

Note The following is the correct file format:

[BuildingName], [FloorName], [AP/WiFi TDOA Receiver/Chokepoint Name], (aAngle), (bAngle), [X], [Y], ([aAngleElevation, bAngleElevation, Z]), (aAntennaType, aAntennaMode, (aAntennaPattern, (aAntennaGain)), bAntennaType, bAntennaDiversity, (bAntennaPattern, bAntennaGain)))))

The parameters in square brackets are mandatory, and those in parentheses are optional.

Note Angles must be entered in radians (X,Y), and the height is entered in feet. The aAngle and bAngle range is from –2Pi (-6.28...) to 2Pi (6.28...), and the elevation ranges from –Pi (-3.14...) to Pi (3.14...).

Step 8 Click **Import**. The RF calculation takes approximately two seconds per component.

Changing Access Point Positions by Importing and Exporting a File

You can change an access point position by importing or exporting a file. The file contains only the lines describing the access point you want to move. This option takes less time than manually changing multiple access point positions. To change access point positions using the importing or exporting of a file, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 From the Select a command drop-down list, choose Import AP/WiFi TDOA Receiver/Chokepoint Placement or Export AP/WiFi TDOA Receiver/Chokepoint Placement, and click **Go**.

Step 3 In Import Data from File or Export Data from File, click **Browse** to find the file you want to import. The file in the [BuildingName], [FloorName], [APName], (aAngle), (bAngle), [X], [Y], ([aAngleElevation, bAngleElevation, Z]), (aAntennaType, aAntennaMode, (aAntennaPattern, (aAntennaGain)), bAntennaType, bAntennaDiversity, (bAntennaPattern, bAntennaGain))))) format must already be created and added to NCS. (See the "Inspecting VoWLAN Readiness" section on page 4-79.)

Note The parameters in square brackets are mandatory, and those in parentheses are optional.

Note Angles must be entered in radians (X,Y), and the height is entered in feet. The aAngle and bAngle range is from –2Pi (-6.28...) to 2Pi (6.28...), and the elevation ranges from –Pi (-3.14...) to Pi (3.14...).

Step 4 Click **Import**. The RF calculation takes approximately two seconds per access point.

Configuring ChokePoints

Using chokepoints in conjunction with active compatible extensions compliant tags provides immediate location information on a tag and its asset. When a Cisco Compatible Extension tag moves out of the range of a chokepoint, its subsequent beacon frames do not contain any identifying chokepoint information. Location determination of the tag defaults to the standard calculation methods based on RSSIs reported by the access point associated with the tag.

This section contains the following topics:

Using Chokepoints to Enhance Tag Location Reporting

Installation of chokepoints provides enhanced location information for RFID tags. When an active Cisco Compatible Extensions Version 1-compliant RFID tag enters the range of a chokepoint, it is stimulated by the chokepoint. The MAC address of this chokepoint is then included in the next beacon sent by the stimulated tag. All access points that detect this tag beacon then forward the information to the controller and location appliance.

Using chokepoints in conjunction with active compatible extensions compliant tags provides immediate location information on a tag and its asset. When a Cisco Compatible Extension tag moves out of the range of a chokepoint, its subsequent beacon frames do not contain any identifying chokepoint information. Location determination of the tag defaults to the standard calculation methods based on RSSIs reported by the access point associated with the tag.

Adding Chokepoints to the NCS Database

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be entered into the location database and plotted on an NCS map.

To add a chokepoint to the NCS database, follow these steps:

Step 1 Choose **Configure > Chokepoints**.

Step 2 From the Select a command drop-down list, choose **Add Chokepoints**.

Step 3 Click **Go**.

Step 4 Enter the MAC address and name for the chokepoint.

Step 5 Select the **Entry/Exit Chokepoint** check box.

Step 6 Enter the coverage range for the chokepoint.

Note The Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 7 Click **OK**.

Note After the chokepoint is added to the database, it can be placed on the appropriate NCS floor map.

Adding a Chokepoint to an NCS Map

To add the chokepoint to a map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 In the Maps page, choose the link that corresponds to the floor location of the chokepoint.

Step 3 From the Select a command drop-down list, choose **Add Chokepoints**.

Step 4 Click **Go**.

Note The Add Chokepoints summary page lists all recently added chokepoints that are in the database but are not yet mapped.

Step 5 Select the check box next to the chokepoint that you want to place on the map.

Step 6 Click **OK**.

A map appears with a chokepoint icon located in the top left-hand corner. You are now ready to place the chokepoint on the map.

Step 7 Left-click the chokepoint icon and drag it to the proper location.

Note The MAC address, name, and coverage range of the chokepoint appear in the dialog box in the left when you click the chokepoint icon for placement.

Step 8 Click **Save**.

You are returned to the floor map and the added chokepoint appears on the map.

Note The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.

Note The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

Note The MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint appear when you hover your mouse cursor over its map icon.

Step 9 If the chokepoint does not appear on the map, select the **Chokepoints** check box located in the Floor Settings menu.

Note Do not click **Save Settings** unless you want to save this display criteria for all maps.

Note You must synchronize network design to the mobility services engine or location server to push chokepoint information.

Positioning Chokepoints

To position chokepoints on the map, follow these steps:

Step 1 Left-click the **Chokepoint** icon and drag it to the proper location.

Note The MAC address, name, and coverage range of the chokepoint appear in the dialog box in the left when you click the chokepoint icon for placement.

Step 2 Click **Save** when the icon is correctly placed on the map.

Step 3 The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor. If the icon does not appear, repeat Step 11.

Note The rings around the chokepoint icon indicate the coverage area. When a Cisco Compatible Extensions tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. The chokepoint range is provided as a visual only, but chokepoint vendor software is required to actually configure the range. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

Note The MAC address, name, and range of a chokepoint are displayed when you hover your mouse cursor over its map icon.

Step 4 If the chokepoint does not appear on the map, choose **Layers** to view a drop-down list of possible elements to display on the map. Select the **Chokepoints** check box.

Step 5 Click **X** to close the Layers page.

Note Do not click **Save Settings** unless you want to save this display criteria for all maps.

Note You can change the position of chokepoints by importing or exporting a file. See the "Positioning Access Points, Wi-Fi TDOA Receivers, and Chokepoints by Importing or Exporting a File" section on page 4-56 for more information.

Removing Chokepoints from the NCS Database and Map

You can remove one or multiple chokepoints at a time.

To delete a chokepoint, follow these steps:

Step 1 Choose **Configure > Chokepoints**:

Step 2 Select the box(es) next to the chokepoint(s) to be deleted.

Step 3 From the Select a command drop-down list, choose **Remove Chokepoints**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the chokepoint deletion.

Step 6 From the Select a command drop-down list in the applicable NCS floor map page, choose **Remove Chokepoints**.

Step 7 Click **Go**.

Step 8 Select the check box(es) next to the chokepoint(s) to be deleted.

Step 9 Click **OK**.

Configuring Wi-Fi TDOA Receivers

This section contains the following topics:

Adding Wi-Fi TDOA Receivers to the NCS Database

To add Wi-Fi TDOA receivers to the NCS database, follow these steps:

Step 1 Choose **Configure > WiFi TDOA Receivers**.

Step 2 From the Select a command drop-down list, choose **Add WiFi TDOA Receivers**.

Step 3 Click **Go**.

Step 4 Enter the MAC address, name, and static IP address for the Wi-Fi TDOA receiver.

Note Wi-Fi TDOA receivers are configured separately using the Wi-Fi TDOA receiver vendor software.

Step 5 Click **OK** to save the Wi-Fi TDOA receiver entry to the database.

Note After the Wi-Fi TDOA receiver is added to the database, place it on the appropriate NCS floor map. See the "Adding Wi-Fi TDOA Receivers to the NCS Database" section on page 4-62 for more information.

Adding Wi-Fi TDOA Receivers to a Map

To add a **WiFi TDOA** receiver to a map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Choose the link that corresponds to the floor location of the Wi-Fi TDOA receiver.

Step 3 From the Select a command drop-down list, choose **Add WiFi TDOA Receivers**.

Step 4 Click **Go**.

Note The Add WiFi TDOA Receivers summary page lists all recently added Wi-Fi TDOA receivers that are in the database but are not yet mapped.

Step 5 Select the check box next to the Wi-Fi TDOA receiver to be added to the map.

Step 6 Click **OK**.

A map appears with a green WiFi TDOA receiver icon located in the top left-hand corner. You are now ready to position the Wi-Fi TDOA receiver on the map.

Positioning Wi-Fi TDOA Receivers

To position Wi-Fi TDOA receivers on the map, follow these steps:

Step 1 Left-click the **WiFi TDOA receiver** icon and drag it to the proper location.

Note The MAC address and name of the Wi-Fi TDOA receiver appear in the left pane when you click the WiFi TDOA receiver icon for placement.

Step 2 Click **Save** when the icon is correctly placed on the map.

Note The MAC address of the Wi-Fi TDOA receiver appears when you hover your mouse cursor over its map icon.

Step 3 If the chokepoint does not appear on the map, click **Layers** to view a drop-down list of possible elements to display on the map. Select the **WiFi TDOA Receivers** check box.

Step 4 Click **X** to close the Layers page.

Note Do not select **Save Settings** unless you want to save this display criteria for all maps.

Note You can change the position of Wi-Fi TDOA Receivers by importing or exporting a file. See the "Positioning Access Points, Wi-Fi TDOA Receivers, and Chokepoints by Importing or Exporting a File" section on page 4-56 for more information.

Removing Wi-Fi TDOA Receivers from the Map

To remove a Wi-Fi TDOA receiver from a floor map, follow these steps:

Step 1 From the Select a command drop-down list in the applicable NCS floor map page, choose **Remove WiFi TDOA Receivers**.

Step 2 Click **Go**.

Step 3 Select the check box(es) next to the Wi-Fi TDOA receiver(s) to be deleted.

Note You can remove multiple Wi-Fi TDOA receivers at a time from a map.

Step 4 Click **OK**.

Removing Wi-Fi TDOA Receivers from the NCS Database

To remove a Wi-Fi TDOA receiver from the NCS database, follow these steps:

Step 1 Choose **Configure > WiFi TDOA Receivers**.

Step 2 Select the check box(es) next to the Wi-Fi TDOA receiver(s) to be deleted.

Note You can remove multiple Wi-Fi TDOA receivers at a time from the database.

Step 3 From the Select a command drop-down list, choose **Remove WiFi TDOA Receivers**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Managing RF Calibration Models

If the provided RF models do not sufficiently characterize the floor layout, you can create a calibration model that is applied to the floor and better represents the attenuation characteristics of that floor. The calibration models are used as RF overlays with measured RF signal characteristics that can be applied to different floor areas. This enables the Cisco WLAN solution installation team to lay out one floor in a multi-floor area, use the RF calibration tool to measure, save the RF characteristics of that floor as a new calibration model, and apply that calibration model to all the other floors with the same physical layout.

You can collect data for a calibration using one of two methods:

- Point mode data collection—Calibration points are selected and their coverage area is calculated one location at a time.
- Linear mode data collection—A series of linear paths are selected and then calculated as you traverse the path. This approach is generally faster than the point mode data collection. You can also employ point mode data collection to augment data collection for locations missed by the linear paths.

Note Calibration models can only be applied to clients, rogue clients, and rogue access points. Calibration for tags is done using the Aeroscout System Manager. See the following URL for details on tag calibration at: http://support.aeroscout.com.

Note We recommend client device that supports both 802.11a/n and 802.11b/g/n radios to expedite the calibration process for both spectrums.

Use a laptop or other wireless device to open a browser to the NCS server and perform the calibration process.

This section contains the following topics:

- Apply the Model to the Floor, page 4-69
- Deleting Calibration Models, page 4-69

Accessing Current Calibration Models

To access current calibration models, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 From the Select a command drop-down list, choose **RF Calibration Models**. The Model Name and Status for each calibration model are listed.

Step 3 Click the model name to access a specific calibration model.

Applying Calibration Models to Maps

To apply a current calibration model to a map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 From the Select a command drop-down list, choose **RF Calibration Models**.

Step 3 Click the model name to access the applicable calibration model.

Step 4 From the Select a command drop-down list, choose **Apply to Maps**.

Step 5 Click **Go**.

Viewing Calibration Model Properties

To view or edit current calibration models, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 From the Select a command drop-down list, choose **RF Calibration Models**.

Step 3 Click the model name to access the applicable calibration model.

Step 4 From the Select a command drop-down list, choose **Properties**.

Step 5 Click **Go** to view or edit calibration model details. See the "Viewing Calibration Model Properties" section on page 4-65 for more information.

Viewing Calibration Model Details

To edit calibration model details, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 From the Select a command drop-down list, choose **RF Calibration Models**.

Step 3 Click the model name to access the applicable calibration model.

Step 4 From the Select a command drop-down list, choose **Properties**.

Step 5 Click **Go**.

Step 6 The following parameters might be edited:

- Sweep Client Power for Location—Click to enable. You might want to enable this if a high density of access points exists and transmit power is reduced or unknown. The sweeping range of client transmit power might improve accuracy but scalability is negatively affected.
- HeatMap Binsize—Choose **4**, **8**, **16**, or **32** from the drop-down list.
- HeatMap Cutoff—Determine the heatmap cutoff. We recommend a low heatmap cutoff especially if the access point density is high and RF propagation conditions are favorable. A higher cutoff value increases scalability but might cause difficulty when locating clients.

Step 7 When any necessary changes have been made or to exit the page, click **OK**.

Creating New Calibration Models

To create a new calibration model, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 From the Select a command drop-down list, choose **RF Calibration Models**.

Step 3 Click **Go**.

Step 4 From the Select a command drop-down list, choose **Create New Model**.

Step 5 Click **Go**.

Step 6 Enter a model name, and click **OK**.

The new model appears along with the other RF calibration models with a status of Not Yet Calibrated.

Starting Calibration Process

To start the calibration process, follow these steps:

Step 1 Click the model name to open the Calibration Model > Model Name page.

Step 2 From the Select a command drop-down list, choose **Add Data Points**.

Step 3 Click **Go**.

Step 4 Enter the MAC address of the device being used to perform the calibration. Manually-entered MAC addresses must be delimited with colons (such as FF:FF:FF:FF:FF:FF).

Note If this process is being performed from a mobile device connected to the NCS through the Cisco Centralized architecture, the MAC address text box is automatically populated with the device address.

Step 5 Choose the appropriate campus, building, floor, or outdoor area where the calibration is performed.

Note The calibration in the outdoor area is supported in Release 1.0.x and later. You can use this option to add the calibration data points to the outdoor area. The data points can be added to the outdoor area using the same procedure for calibration.

Step 6 Click **Next**.

Step 7 When the chosen floor map and access point locations appear, a grid of plus marks (+) indicates the locations where data collection for calibration is performed.

Using these locations as guidelines, you can perform either a point or linear collection of data by appropriate placement of either the Calibration Point pop-up (point) or the Start and Finish pop-ups (linear) that appear on the map when the respective options are displayed.

If you want to perform a point collection of data for the calibration, do the following:

a. Choose **Point** from the Collection Method drop-down list and select the **Show Data points** check box if not already selected. A calibration point pop-up appears on the map.

b. Position the tip of the calibration point pop-up at a data point (+), and click **Go**. A dialog box appears showing the progress of the data collection.

Note Rotate the calibrating client laptop during data collection so that the client is heard evenly by all access points in the vicinity.

c. When the data collection is complete for a selected data point and the coverage area is plotted on the map, move the calibration point pop-up to another data point, and click **Go**.

Note The coverage area plotted on the map is color-coded and corresponds with the specific wireless LAN standard used to collect that data. Information on color-coding is provided in legend on the left side of the page. Additionally, the progress of the calibration process is indicated by two status bars above the legend, one for 802.11a/n and one for 802.11b/g/n.

Note To delete data points for locations selected in error, click **Delete** and move the black square that appears over the appropriate data points. Resize the square as necessary by pressing **Ctrl** and moving the mouse.

d. Repeat point collection Steps a. to c. until the calibration status bar of the relevant spectrums (802.11a/n, 802.11b/g/n) display as ‘done.’

Note The calibration status bar indicates data collection for the calibration as done after roughly 50 distinct locations and 150 measurements have been gathered. For every location point saved in the calibration process, more than one data point is gathered. The progress of the calibration process is indicated by two status bars above the legend, one for 802.11b/g/n and one for 802.11a/n.

If you want to perform a linear collection of data for the calibration, do the following:

a. Choose **Linear** from the Collection Method drop-down list, and select the **Show Data points** check box if not already selected. A line appears on the map with both Start and Finish pop-ups.

b. Position the tip of the Start pop-up at the starting data point.

c. Position the Finish pop-up at the ending data point.

d. Position yourself with your laptop at the starting data point, and click **Go**. Walk steadily towards the end point along the defined path. A dialog box appears to show that data collection is in process.

Note Do not stop data collection until you reach the end point even if the data collection bar indicates completion.

Note Only Intel and Cisco adapters have been tested. Make sure Enable Cisco Compatible Extensions and Enable Radio Management Support are enabled in the Cisco Compatible Extension Options.

e. Press the space bar (or Done on the data collection panel) when you reach the end point. The collection pane displays the number of samples taken before it closes to reveal the map. The map displays all the coverage areas where data was collected.

Note To delete data points for locations selected in error, click **Delete** and move the black square that appears over the appropriate data points. Resize the square as necessary by pressing the **Ctrl** and moving the mouse.

Note The coverage area is color-coded and corresponds with the specific wireless LAN standard used to collect that data. Information on color-coding is provided in legend on the left-hand side of the page.

f. Repeat linear collection Steps b to e until the status bar for the respective spectrum is filled in (done).

Note You can augment linear collection with point mode data collection to address missed coverage areas.

Step 8 Click the name of the calibration model at the top of the page to return to the main page for that model to calibrate the data points.

Step 9 Choose **Calibrate** from the Select a command drop-down list, and click **Go**.

Step 10 Click the **Inspect Location Quality** link when calibration completes. A map displays showing RSSI readings displays.

Step 11 To use the newly created calibration model, you must apply the model to the floor on which it was created (and on any other floors with similar attenuation characteristics as well). Choose **Monitor > Site Maps** and find the specific floor to which the model is applied. At the floor map interface, choose **Edit Floor Area** from the drop-down list, and click **Go**.

Step 12 From the Floor Type (RF Model) drop-down list, choose the newly created calibration model. Click **OK** to apply the model to the floor.

Note This process can be repeated for as many models and floors as needed. After a model is applied to a floor, all location determination performed on that floor is done using the specific collected attenuation data from the calibration model.

Calibrating

To compute the collected data points, follow these steps:

Step 1 Click the model name to open the Calibration Model > Model Name page.

Step 2 In the Calibration Model > Model Name page, choose **Calibrate** from the Select a command drop-down list.

Step 3 Click **Go**.

Apply the Model to the Floor

To use the newly created calibration model, you must apply the model to the floor on which it was created (along with other floors with similar attenuation characteristics).

To apply the model to the floor, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Locate the specific floor to which the model is applied.

Step 3 From the Select a command drop-down list, choose **Edit Floor Area**.

Step 4 Click **Go**.

Step 5 From the Floor Type (RF Model) drop-down list, choose the newly-created calibration model.

Step 6 Click **OK** to apply the model to the floor.

This process can be repeated for as many models and floors as needed. After a model is applied to a floor, all location determination performed on that floor is done using the specific collected attenuation data from the calibration model.

Deleting Calibration Models

To delete a calibration model, follow these steps:

Step 1 Click the model name to open the Calibration Model > Model Name page.

Step 2 From the Select a command drop-down list, choose **Delete Model**.

Step 3 Click **Go**.

Managing Location Presence Information

You can enable location presence through mobility services engine to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by clients on a demand basis for use by location-based services and applications. See the "Enabling Location Presence for Mobility Services" section on page 11-54 for more information on enabling location presence.

To view or edit current location presence information for a current map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Select the check box of the map.

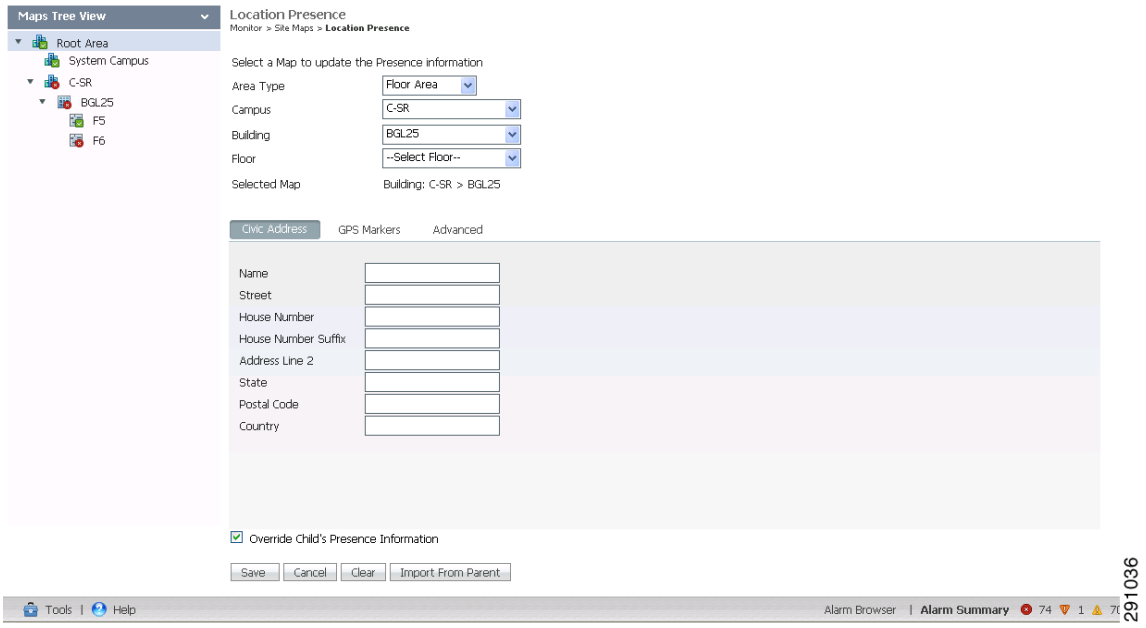
Step 3 From the Select a command drop-down list, choose **Location Presence**.

Step 4 Click **Go**.

The Location Presence page appears. (See Figure 4-28).

Note The current map location information (Area Type, Campus, Building, and Floor) see the map you selected in the **Monitor > Site Maps** page. To select a different map, use the Select a Map to Update Presence Information drop-down lists to choose the new map location.

Figure 4-28 Location Presence



Step 5 Click the **Civic Address**, **GPS Markers**, or **Advanced** tab.

- Civic Address—Identifies the campus, building, or floor by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
- GPS Markers—Identify the campus, building, or floor by longitude and latitude.

– Advanced—Identifies the campus, building, or floor with expanded civic information such as neighborhood, city division, county, and postal community name.

Note Each selected field is inclusive of all of those above it. For example, if you select Advanced, it can also provide GPS and Civic location information upon client demand. The selected setting must match what is set on the mobility services engine level. See the Enabling Location Presence for Mobility Services, page 11-54 for more information.

Note If a client requests location information such as GPS Markers for a campus, building, floor, or outdoor area that is not configured for that field, an error message appears.

Note By default, the Override Child Element Presence Info check box is selected.

Searching Maps

You can use the following parameters in the Search Maps page:

- Search for
- Map Name
- Search in
- Save Search
- Items per page

After you click **Go**, the map search results page appears (see Table 4-7).

Table 4-7 Map Search Results

Field	Options
Name	Clicking an item in the Name column provides a map of an existing building with individual floor area maps for each floor.
Type	Campus, building, or floor area.
Total APs	Displays the total number of Cisco Radios detected.
a/n Radios	Displays the number of 802.11a/n Cisco Radios.
b/g/n Radios	Displays the number of 802.11b/g/n Cisco Radios.

Using the Map Editor

You can use the NCS map editor to define, draw, and enhance floor plan information. This section contains the following topics:

Opening the Map Editor

Follow these steps to use the map editor:

Step 1 Choose **Monitor > Site Maps** to display the Maps page.

Step 2 Click the desired campus. The Site Maps > Campus Name page appears.

Step 3 Click a campus and then click a building.

Step 4 Click the desired floor area. The Site Maps > Campus Name > Building Name > Floor Area Name page appears.

Step 5 From the Select a command drop-down list, choose **Map Editor**, and click **Go**. The Map Editor page appears.

Note Make sure that the floor plan images are properly scaled so that all white space outside of the external walls is removed. To make sure that floor dimensions are accurate, click the **compass tool** on the toolbar.

Step 6 Position the reference length. When you do, the Scale menu appears with the line length supplied. Enter the dimensions (width and height) of the reference length, and click **OK**.

Step 7 Determine the propagation pattern from the Antenna Mode drop-down list.

Step 8 Make antenna adjustments by sliding the antenna orientation bar to the desired degree of direction.

Step 9 Choose the desired access point.

Step 10 Click **Save**.

Using the Map Editor to Draw Polygon Areas

If you have a building that is non-rectangular or you want to mark a non-rectangular area within a floor, you can use the map editor to draw a polygon-shaped area.

Step 1 Add the floor plan if it is not already represented in NCS (see the "Adding Floor Areas to a Campus Building" section on page 4-28).

Step 2 Choose **Monitor > Site Maps**.

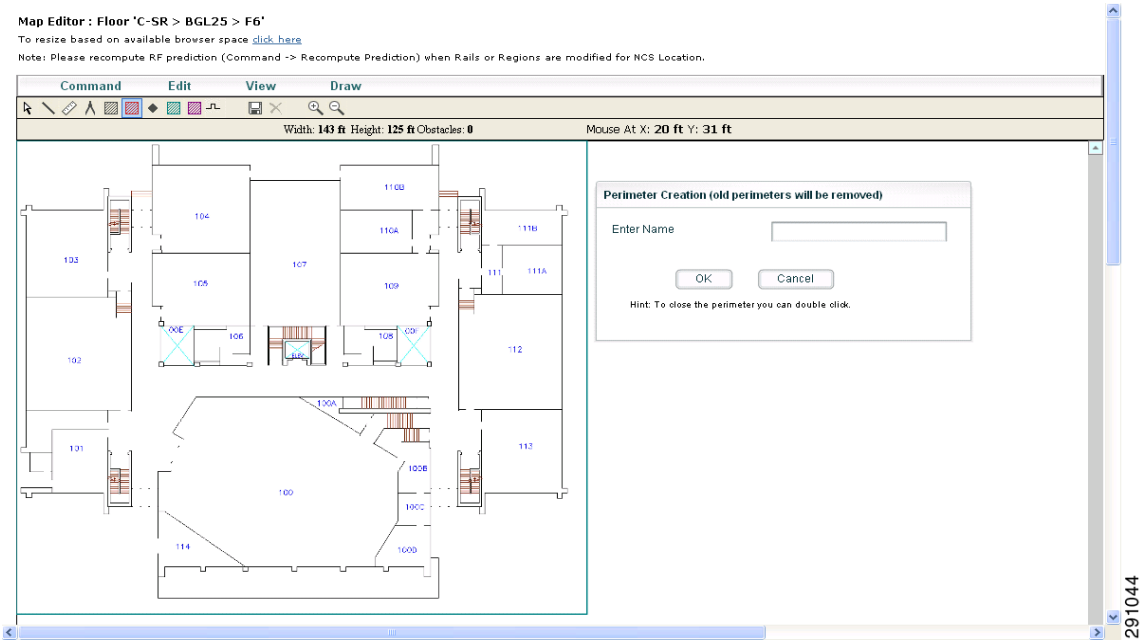
Step 3 Click the Map Name that corresponds to the outdoor area, campus, building, or floor you want to edit.

Step 4 From the Select a command drop-down list, choose **Map Editor**, and click **Go**.

Step 5 It the Map Editor page, click the **Add Perimeter** icon on the toolbar (see Figure 4-29).

A pop-up appears.

Figure 4-29 Map Editor Page



Step 6 Enter the name of the area that you are defining. Click **OK**.

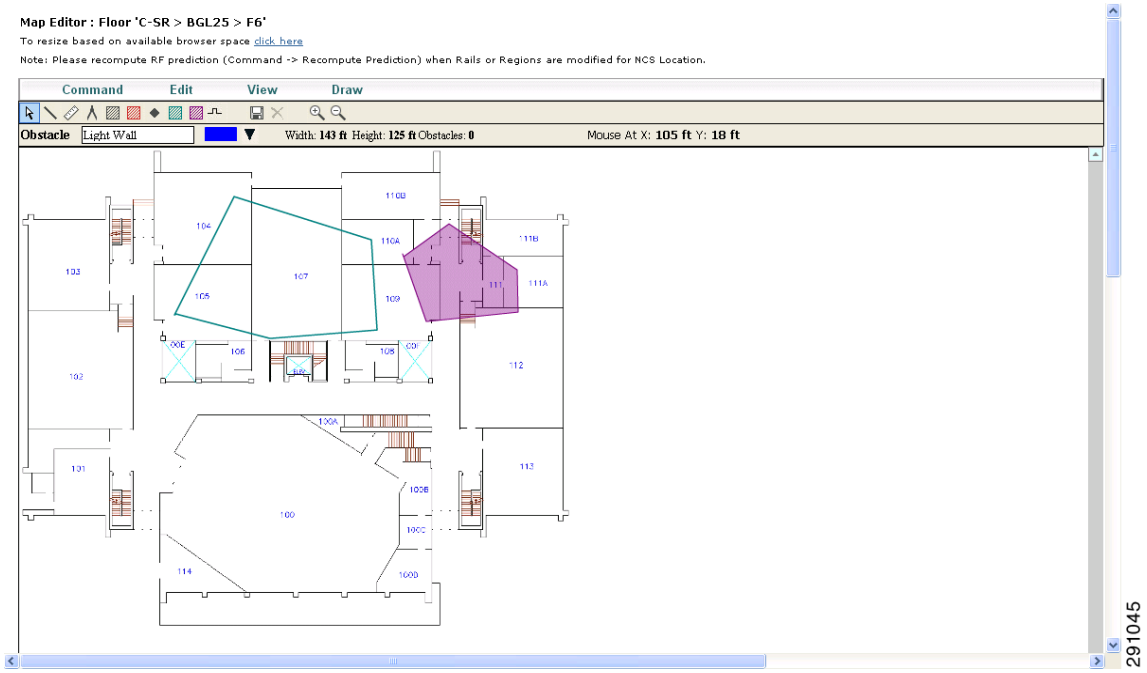
A drawing tool appears.

Step 7 Move the drawing tool to the area you want to outline.

- Click the left mouse button to begin and end drawing a line.
- When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page (see Figure 4-30).

The outlined area must be a closed object to appear highlighted on the map.

Figure 4-30 Polygon Area



Step 8 Click the disk icon on the toolbar to save the newly drawn area.

Step 9 Choose **Command > Exit** to close the window. You are returned to the original floor plan.

Note When you return to the original floor plan view after exiting the map editor, the newly drawn area is not visible; however, it appears in the Planning Model page when you add elements.

Step 10 Choose **Planning Mode** from the Select a command drop-down list to begin adding elements to the newly defined polygon-shaped area.

The Table 4-8 describes the obstacle color coding.

Table 4-8 Obstacle Color Coding

Type of obstacle	Color coding	Loss (in dB)
Thick wall		13
Light wall		2
Heavy door		15
Light door		4
Cubicle		1
Glass		1.5

Note The RF prediction heatmaps for access points approximates of the actual RF signal intensity. It takes into account the attenuation of obstacles drawn using the Map Editor but it does not take into account the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions. The thick wall (color-coded orange) with a loss of 13 dB might not be enough to contain the RF signal beyond the walls of the heatmap.

Defining an Inclusion Region on a Floor

To define an inclusion area, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the name of the appropriate floor area.

Step 3 From the Select a command drop-down list, choose **Map Editor**.

Step 4 Click **Go**.

Step 5 At the map, click the aqua box on the toolbar.

Note A message box appears reminding you that only one inclusion area can be defined at a time. Defining a new inclusion region automatically removes the previously defined inclusion region. By default, an inclusion region is defined for each floor when it is added to the NCS. The inclusion region is indicated by a solid aqua line and generally outlines the region.

Step 6 Click **OK** in the message box that appears. A drawing icon appears to outline the inclusion area.

Step 7 To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.

Step 8 Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.

Step 9 Repeat Step 8 until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area.

Step 10 Choose **Save** from the Command menu or click the **disk** icon on the toolbar to save the inclusion region.

Note If you made an error in defining the inclusion area, click the area. The selected area is outlined by a dashed aqua line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.

Step 11 To return to the floor map to enable inclusion regions on heatmaps, choose **Exit** from the Command menu.

Step 12 Select the **Location Regions** check box if it is not already selected. If you want it to apply to all floor maps, click **Save settings**. Close the Layers configuration page.

Step 13 To resynchronize the NCS and MSE databases, choose **Services > Synchronize Services**.

Note If the two DBs are already synchronized then a resynchronization happens automatically every time there is a change. There is no need for an explicit resynch.

Step 14 In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Note Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

Defining an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are generally defined within the borders of an inclusion area.

To define an exclusion area, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the name of the appropriate floor area.

Step 3 From the Select a command drop-down list, choose **Map Editor**.

Step 4 Click **Go**.

Step 5 At the map, click the purple box on the toolbar.

Step 6 Click **OK** in the message box that appears. A drawing icon appears to outline the exclusion area.

Step 7 To begin defining the exclusion area, move the drawing icon to the starting point on the map, and click once.

Step 8 Move the drawing icon along the boundary of the area you want to exclude. Click once to start a boundary line, and click again to end the boundary line.

Step 9 Repeat Step 8 until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is completely defined. The excluded area is shaded in purple.

Step 10 To define additional exclusion regions, repeat Step 5 to Step 9.

Step 11 When all exclusion areas are defined, choose **Save** from the Command menu or click the **disk** icon on the toolbar to save the exclusion region.

Note To delete an exclusion area, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.

Step 12 To return to the floor map to enable exclusion regions on heatmaps, choose **Exit** from the Command menu.

Step 13 Select the **Location Regions** check box if it is not already selected, click **Save setting**s, and close the Layers configuration page when complete.

Step 14 To resynchronize the NCS and location databases, choose **Services > Synchronize Services**.

Step 15 In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Defining a Rail Line on a Floor

You can define a rail line on a floor that represents a conveyor belt. Additionally, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority).

Note Rail line configurations do not apply to tags.

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

To define a rail with a floor, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the name of the appropriate floor area.

Step 3 Choose **Map Editor** from the Select a command drop-down list.

Step 4 Click **Go**.

Step 5 In the map, click the **rail** icon (to the right of the purple exclusion icon) on the toolbar.

Step 6 In the message dialog box that appears, enter a snap-width (feet or meters) for the rail and then click **OK**. A drawing icon appears.

Step 7 Click the **drawing** icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.

Step 8 Click the **drawing** icon twice when the rail line is completely drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.

Note To delete a rail line, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the X icon on the toolbar. The area is removed from the floor map.

Step 9 To return to the floor map to enable rails on heatmaps, choose **Exit** from the Command menu.

Step 10 At the floor map, choose the **Layers** drop-down list.

Step 11 Select the **Rails** check box for if it is not already selected, click **Save settings**, and close the Layers configuration panel when complete.

Step 12 To resynchronize the NCS and mobility services engine, choose **Services > Synchronize Services**.

Step 13 In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Inspecting Location Readiness and Quality

You can configure the NCS to verify the ability of the existing access point deployment to estimate the true location of a client, rogue client, rogue access point, or tag within 10 meters at least 90% of the time. The location readiness calculation is based on the number and placement of access points.

You can also check the location quality and the ability of a given location to meet the location specification (10 m, 90%) based on data points gathered during a physical inspection and calibration.

Inspecting Location Readiness

The Inspect Location Readiness feature is a distance-based predictive tool that can point out problem areas with access point placement.

To access the Inspect Location Readiness tool, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the applicable floor area name to view the map.

Note If RSSI is not displayed, you can enable AP Heatmaps by selecting the AP Heatmaps check box on the left sidebar menu.

Note If clients, tags, and access points are not displayed, verify that their respective check boxes are selected on the left sidebar menu. Licenses for both clients and tags must also be purchased for each to be tracked.

Step 3 From the Select a command drop-down list, choose **Inspect Location Readiness**.

Step 4 Click **Go**.

A color-coded map appears showing those areas that meet (indicated by Yes) and do not meet (indicated by No) the ten meter, 90% location specification.

Inspecting Location Quality Using Calibration Data

After completing a calibration model based on data points generated during a physical tour of the area, you can inspect the location quality of the access points.

To inspect location quality based on calibration, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Choose **RF Calibration Model** from the Select a command list. Click **Go**.

A list of calibration models appears.

Step 3 Click the appropriate calibration model.

Details on the calibration including date of last calibration, number of data points by signal type (802.11a, 802.11 b/g) used in the calibration, location, and coverage are displayed.

Step 4 In the same page, click the **Inspect Location Quality** link found under the Calibration Floors heading.

A color-coded map noting percentage of location errors appears.

Note You can modify the distance selected to see the effect on the location errors.

Inspecting VoWLAN Readiness

The VoWLAN Readiness (voice readiness) tool allows you to check the RF coverage to determine if it is sufficient for your voice needs. This tool verifies RSSI levels after access points have been installed.

To access the VoWLAN Readiness Tool (VRT), follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the applicable floor area name.

Step 3 From the Select a command drop-down list, choose **Inspect VoWLAN Readiness**.

Step 4 Choose the applicable **Band**, **AP Transmit Power**, and **Client** parameters from the drop-down lists.

Note By default, the region map displays the b/g/n band for Cisco Phone-based RSSI threshold. The new settings cannot be saved.

Step 5 Depending on the selected client, the following RSSI values might not be editable:

- Cisco Phone—RSSI values are not editable.
- Custom—RSSI values are editable with the following ranges:
  - Low threshold between -95dBm to -45dBm
  - High threshold between -90dBm to -40dBm

Step 6 The following color schemes indicate whether or not the area is voice ready:

- Green—Yes
- Yellow—Marginal
- Red—No

Note The accuracy of the Green/Yellow/Red regions depends on the RF environment and whether or not the floor is calibrated. If the floor is calibrated, the accuracy of the regions is enhanced.

Troubleshooting Voice RF Coverage Issues

- Floors with either calibration or no calibration data are treated as follows:
  - Set the AP Transmit field to **Max** (the maximum downlink power settings). If the map still shows some yellow or red regions, more access points are required to cover the floor.
  - If the calibrated model shows red or yellow regions (where voice is expected to be deployed) with the AP Transmit field set to Current, increasing the power level of the access points might help.

Monitoring Mesh Networks Using Maps

You can access and view details for the following elements from a mesh network map in the NCS:

- Mesh Link Statistics
- Mesh Access Points
- Mesh Access Point Neighbors

Details on how this information is accessed and displayed for each of these items is detailed in this section. This section contains the following topics:

Monitoring Mesh Link Statistics Using Maps

You can view the SNR for a specific mesh network link, view the number of packets transmitted and received on that link, and initiate a link test in the **Monitor > Site Maps** page.

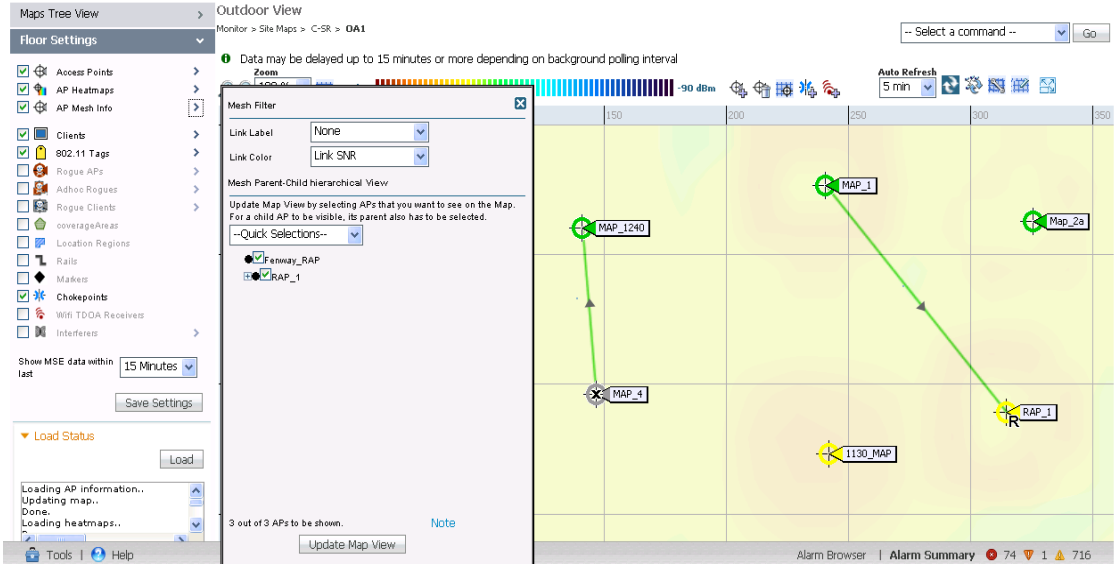
To view details on a specific mesh link between two mesh access points or a mesh access point and a root access point, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the map name that corresponds to the outdoor area, campus, building, or floor you want to monitor.

Step 3 From the left sidebar menu, click the arrow to the right of AP Mesh Info (see Figure 4-31). The Mesh Filter dialog box appears.

Figure 4-31 Mesh Filter Dialog Box



Step 4 Move the cursor over the colored dot next to each mesh access point child to view details on the link between it and its parent. Table 4-9 summarizes the parameters that appear.

The color of the dot also provides a quick reference point of the SNR strength as follows:

- A green dot represents a high SNR (above 25 dB).
- An amber dot represents an acceptable SNR (20-25 dB).
- A red dot represents a low SNR (below 20 dB).
- A black dot indicates a root access point.

The Bridging Link information appears.

Table 4-9 Bridging Link Information

Field	Description
Information fetched on	Date and time that information was compiled.
Link SNR	Link signal-to-noise ratio (SNR).
Link Type	Hierarchical link relationship.
SNR Up	Signal-to-noise radio for the uplink (dB).
SNR Down	Signal-to-noise radio for the downlink (dB).
PER	The packet error rate for the link.
Tx Parent Packets	The TX packets to a node while acting as a parent.
Rx Parent Packets	The RX packets to a node while acting as a parent.
Time of Last Hello	Date and time of last hello.

Step 5 Click either Link Test, Child to Parent or Link Test, Parent to Child. After the link test is complete, a results page appears.

Note A link test runs for 30 seconds.

Note You cannot run link tests for both links (child-to-parent and parent-to-child) at the same time.

Step 6 To view a graphical representation of SNR statistics over a period of time, click the arrow on the link. A page with multiple SNR graphs appears.

The following graphs are displayed for the link:

- SNR Up—Plots the RSSI values of the neighbor from the perspective of the access point.
- SNR Down—Plots the RSSI values that the neighbor reports to the access point.
- Link SNR—Plots a weighed and filtered measurement based on the SNR Up value.
- The Adjusted Link Metric—Plots the value used to determine the least cost path to the root access point. This value represents the ease of getting the rooftop access point and accounts for the number of hops. The lower the ease value, the less likely the path is used.
- The Unadjusted Link Metric—Plots the least cost path to get to the root access point unadjusted by the number of hops. The higher the value for the unadjusted link, the better the path.

Monitoring Mesh Access Points Using Maps

You can view the following summary information for a mesh access point from a mesh network map:

- Parent
- Number of children
- Hop count
- Role
- Group name
- Backhaul interface
- Data Rate
- Channel

Note This information is in addition to the information shown for all access points (MAC address, access point model, controller IP address, location, height of access point, access point uptime, and LWAPP uptime).

Note You can also view detailed configuration, and access alarm, and event information from the map. For detailed information on the Alarms and Events displayed, see the "Alarm and Event Dictionary" section on page 13-1.

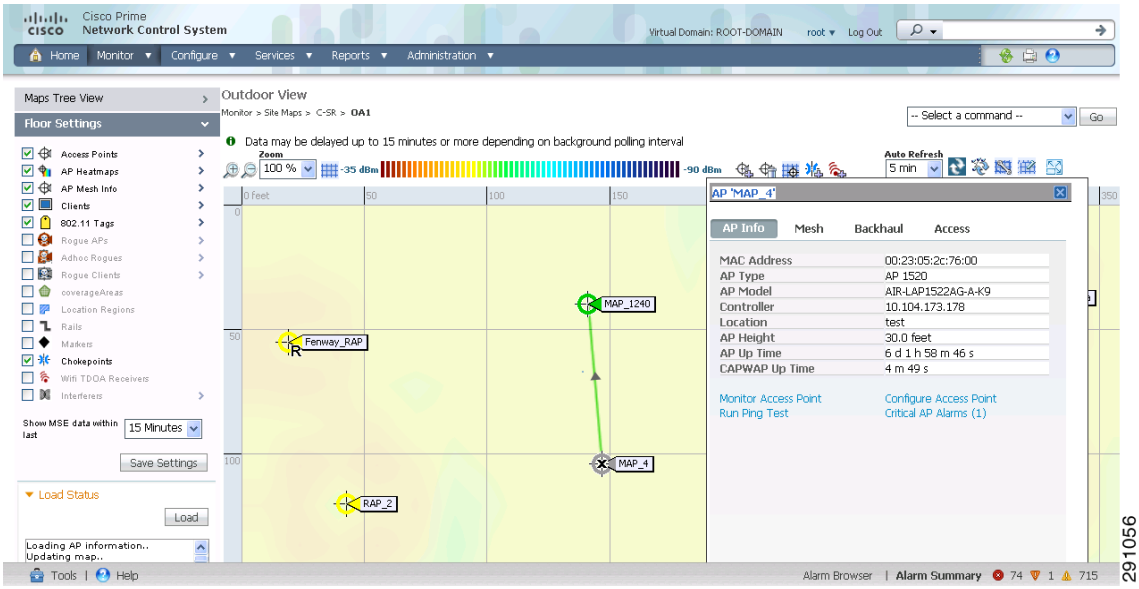
To view summary and detailed configuration information for a mesh access point from a mesh network map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the map name that corresponds to the outdoor area, campus, building, or floor location of the access point you want to monitor.

Step 3 To view summary configuration information for an access point, hover your mouse cursor over the access point that you want to monitor. A dialog box with configuration information for the selected access point appears (see Figure 4-32).

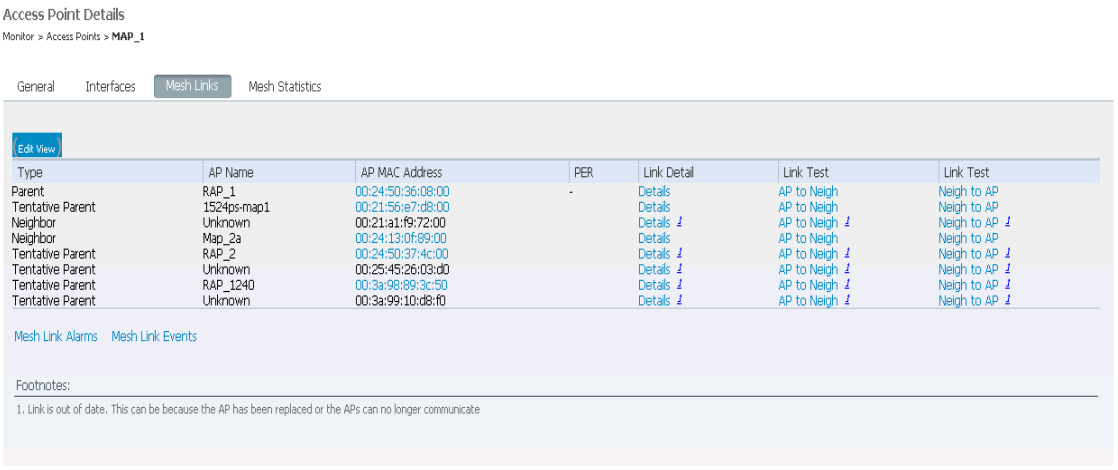
Figure 4-32 Mesh AP Summary Dialog Box



Step 4 To view detailed configuration information for an access point, double-click the access point appearing on the map. The configuration details for the access point appear (see Figure 4-33).

Note For more details on the View Mesh Neighbors link in the access point dialog box (see Figure 4-32), see the "Monitoring Mesh Access Point Neighbors Using Maps" section on page 4-84. If the access point has an IP address, a Run Ping Test link is also visible at the bottom of the mesh access point dialog box.

Figure 4-33 Mesh AP Details Page



Step 5 In the Access Point Details configuration page, follow these steps to view configuration details for the mesh access point:

a. Click the **General** tab to view the overall configuration of the mesh access point such as the AP name, MAC address, AP Up time, associated controllers (registered and primary) operational status, and software version.

Note The software version for mesh access points is appended with the letter *m* and the word *mesh* appears in parentheses.

b. Click the **Interface** tab to view configuration details for the interfaces supported on the mesh access point. Interface options are radio and Ethernet.

c. Click the **Mesh Links** tab to view parent and neighbor details (name, MAC address, packet error rate, and link details) for the mesh access point. You can also initiate link tests from this page.

d. Click the **Mesh Statistics** tab to view details on the bridging, queue, and security statistics for the mesh access point. For more details on mesh statistics, see the "Mesh Statistics Tab" section on page 5-82.

Monitoring Mesh Access Point Neighbors Using Maps

To view details on neighbors of a mesh access point from a mesh network map, follow these steps:

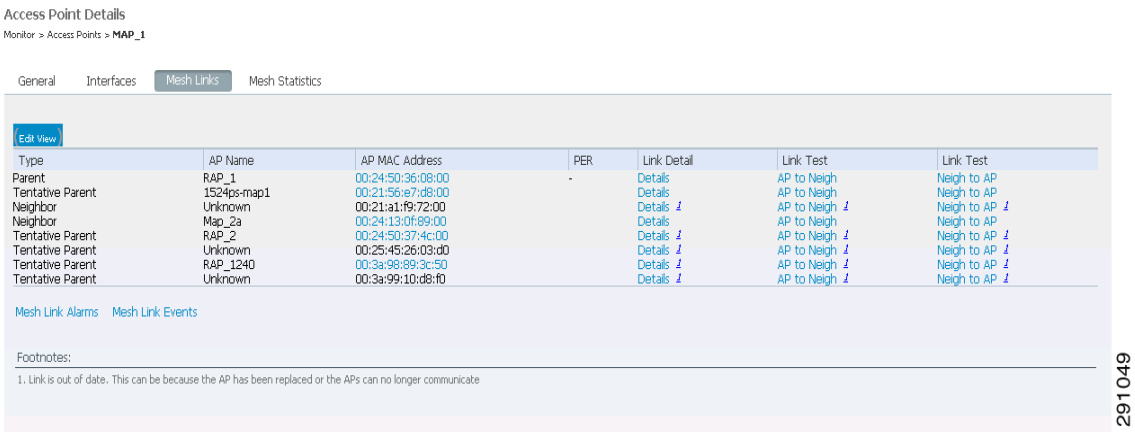
Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the map name that corresponds to the outdoor area, campus, building, or floor you want to monitor.

Step 3 To view detailed information on mesh links for a mesh access point, click the arrow portion of the access point label. The Access Points page appears.

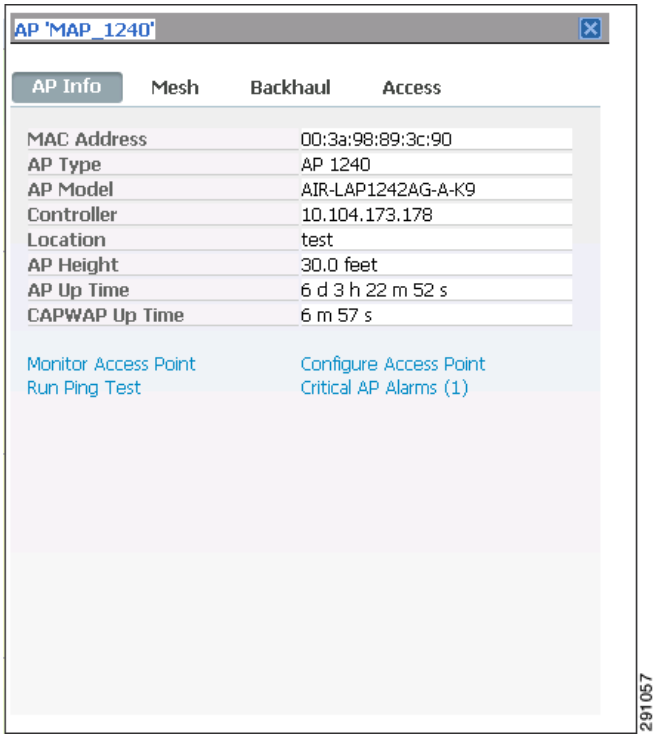
Step 4 Click the **Mesh Links** tab (see Figure 4-34).

Figure 4-34 Access Points > Mesh Links Page



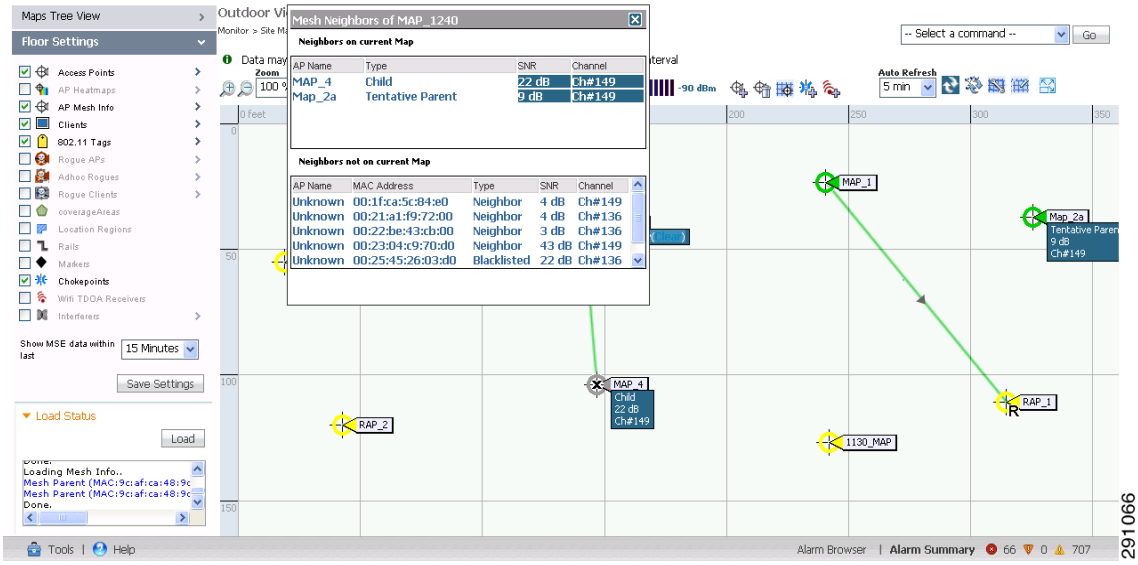
Note You can also view mesh link details for neighbors of a selected access point by clicking the **View Mesh Neighbors** link on the Mesh tab of the access point configuration summary dialog box, which appears when you hover your mouse cursor over an access point on a map (see Figure 4-35).

Figure 4-35 Access Point Configuration Summary Dialog Box



Note Signal-to-noise (SNR) appears in the View Mesh Neighbors dialog box (see Figure 4-36).

Figure 4-36 View Mesh Neighbors Dialog Box



Note In addition to listing the current and past neighbors in the dialog box that appears, labels are added to the mesh access points map icons to identify the selected access point, the neighbor access point, and the child access point. Click the **clear** link of the selected access point to remove the relationship labels from the map.

Note The drop-down lists at the top of the mesh neighbors page indicate the resolution of the map (100%) displayed and how often the information displayed is updated (every 5 mins). You can modify these default values.

Viewing the Mesh Network Hierarchy

You can view the parent-child relationship of mesh access points within a mesh network in an easily navigable display. You can also filter which access points are displayed in the map view by selecting only access points of interest.

To view the mesh network hierarchy for a selected network, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

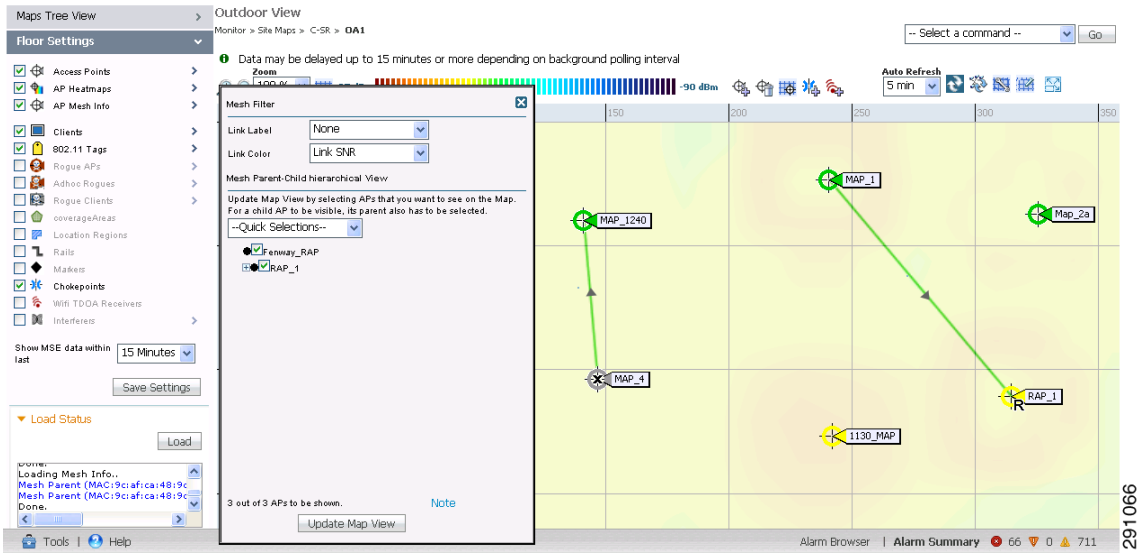
Step 2 Click the map name you want to display.

Step 3 Select the **AP Mesh Info** check box in the left sidebar menu if it is not already selected.

Note The AP Mesh Info check box is only selectable if mesh access points are present on the map. It must be selected to view the mesh hierarchy.

Step 4 Click the blue arrow to the right of the AP Mesh Info to display the Mesh Parent-Child Hierarchical View(see Figure 4-37).

Figure 4-37 Mesh Parent-Child Hierarchical View



Step 5 Click the **plus (+)** sign next to a mesh access point to display its children.

All subordinate mesh access points are displayed when a negative (-) sign appears next to the parent mesh access point entry. For example, in Figure 4-37, the access point, *indoor-mesh-45-rap2*, has only one child, *indoor-mesh-44-map2*.

Step 6 Hover your mouse cursor over the colored dot next to each mesh access point child to view details on the link between it and its parent. Table 4-10 summarizes the parameters that appear.

The color of the dot also provides a quick reference point of the SNR strength:

- A green dot represents a high SNR (above 25 dB).
- An amber dot represents an acceptable SNR (20-25 dB).
- A red dot represents a low SNR (below 20 dB).
- A black dot indicates a root access point.

Table 4-10 Bridging Link Information

Field	Description
Information fetched on	Date and time that information was compiled.
Link SNR	Link signal-to-noise ratio (SNR).
Link Type	Hierarchical link relationship.
SNR Up	Signal-to-noise radio for the uplink (dB).
SNR Down	Signal-to-noise radio for the downlink (dB).
PER	The packet error rate for the link.
Tx Parent Packets	The TX packets to a node while acting as a parent.
Rx Parent Packets	The RX packets to a node while acting as a parent.
Time of Last Hello	Date and time of last hello.

Using Mesh Filters to Modify Map Display of Maps and Mesh Links

In the mesh hierarchical page, you can also define mesh filters to determine which mesh access points display on the map based on hop values as well as what labels display for mesh links.

Mesh access points are filtered by the number of hops between them and their root access point.

To use mesh filtering, follow these steps:

Step 1 To modify what label and color displays for a mesh link, follow these steps:

a. In the Mesh Parent-Child Hierarchical View, choose an option from the Link Label drop-down list. Options are None, Link SNR, and Packet Error Rate.

b. In the Mesh Parent-Child Hierarchical View, choose an option from the Link Color drop-down list to define which parameter (Link SNR or Packet Error Rate) determines the color of the mesh link on the map.

Note The color of the link provides a quick reference point of the SNR strength or Packet Error Rate. Table 4-11 defines the different link colors.

Table 4-11 Definition for SNR and Packet Error Rate Link Color

Link Color	Link SNR	Packet Error Rate (PER)
Green	Represents a SNR above 25 dB (high value)	Represents a PER of one percent (1%) or lower
Amber	Represents a SNR between 20 and 25 dB (acceptable value)	Represents a PER that is less than ten percent (10%) and greater than one percent (1%)
Red	Represents a SNR below 20 dB (low value)	Represents a PER that is greater than ten percent (10%)

Note The Link label and color settings are reflected on the map immediately (see Figure 4-38). You can display both SNR and PER values simultaneously.

Step 2 To modify which mesh access points display based on the number of hops between them and their parents, do the following:

a. In the Mesh Parent-Child Hierarchical View, choose the appropriate options from the Quick Selections drop-down list. A description of the options is provided in Table 4-12.

Table 4-12 Quick Selection Options

Field	Description
Select only Root APs	Choose this setting if you want the map view to display root access points only.
Select up to 1st hops	Choose this setting if you want the map view to display 1st hops only.
Select up to 2nd hops	Choose this setting if you want the map view to display 2nd hops only.
Select up to 3rd hops	Choose this setting if you want the map view to display 3rd hops only.
Select up to 4th hops	Choose this setting if you want the map view to display 4th hops only.
Select All	Select this setting if you want the map view to display all access points.

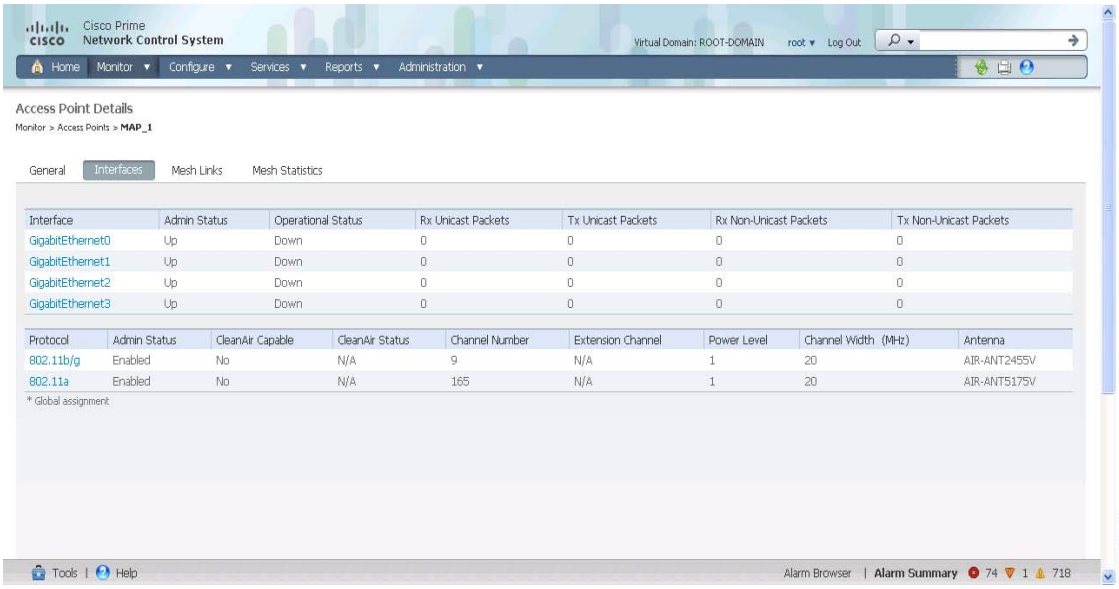
b. Click **Update Map View** to refresh the screen and display the map view with the selected options.

Note Map view information is retrieved from the NCS database and is updated every 15 minutes.

Note You can also select or unselect the check boxes of access points in the mesh hierarchical view to modify which mesh access points are displayed. For a child access point to be visible, the parent access point to root access point must be selected.

Note If you want to have the MAC address appear with the client logo in the Monitor > Site Maps page, follow these steps:
a) Go to the Maps Tree View.
b) Click the > beside Clients.
c) Unselect the **Small Icons** check box.

Figure 4-38 Mesh Filter and Hop Count Configuration Page



Monitoring Tags Using Maps

On an NCS map, you can review the name of the access point that generated the signal for a tagged asset, its strength of signal and when the location information was last updated for the asset. This information is displayed by simply hovering the mouse cursor over the asset tag icon on the map.

To enable tag location status on a map, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Choose **Campus > Building > Floor** for the applicable mobility services engine and tag.

Step 3 Select the **802.11 Tags** check box in the Floor Settings pane (left), if not already selected.

Note Do not click **Save Settings** unless you want to save changes made to the Floor Settings across all maps.

Step 4 Hover the mouse cursor over a tag icon (yellow tag) and a summary of its configuration appears in a dialog box.

Step 5 Click the **tag** icon to see tag details in a new window.

Using Planning Mode

You can calculate the recommended number and location of access points based on whether data and/or voice traffic and/or location are active.

Note Based on the throughput specified for each protocol (802.11a or 802.11 b/g), planning mode calculates the total number of access points required that would provide optimum coverage in your network.

Accessing Planning Mode

To access the Planning Mode feature, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Select the desired campus or building from the Name list.

Step 3 Click the desired floor area in the Building.

Step 4 From the Select a command drop-down list, choose **Planning Mode**.

Step 5 Click **Go**.

Note Planning mode does not use AP type or Antenna pattern information for calculating the number of access points required. The calculation is based on the access point coverage area or the number of users per access point.

Planning Mode options:

- Add APs—Enables you to add access points on a map. See the "Adding Access Points to a Floor Area" section on page 4-34 for details.
- Delete APs—Deletes the selected access points.
- Map Editor—Opens the Map Editor window. See the "Using the Map Editor" section on page 4-71 for more details.
- Synchronize with Deployment—Synchronizes your planning mode access points with the current deployment scenario.
- Generate Proposal—View a planning summary of the current access points deployment.
- Planned AP Association Tool—Allows you to perform add, delete or import an AP Association from an excel or CSV file. Once an access point is defined, it can be associated to a base radio MAC address using the Planned AP Association Tool. If the AP is not discovered they get pushed into a standby bucket and get associated when discovered.

Note AP association is subjected to a limitation that AP should not belong to any floor or outdoor area. If the AP is already assigned to a floor or outdoor area, then the standby bucket holds the AP and when removed from the floor or outdoor, get positioned to the given floor. One Mac address cannot be put into bucket for multiple floor or outdoor areas.

Note The map synchronizations works only if the AP is associated to a base radio MAC address and not to its Ethernet MAC address.

Using Planning Mode to Calculate Access Point Requirements

The NCS planning mode enables you to calculate the number of access points required to cover an area by placing fictitious access points on a map and allowing you to view the coverage area. Based on the throughput specified for each protocol (802.11a/n or 802.11b/g/n), planning mode calculates the total number of access points required to provide optimum coverage in your network. You can calculate the recommended number and location of access points based on the following criteria:

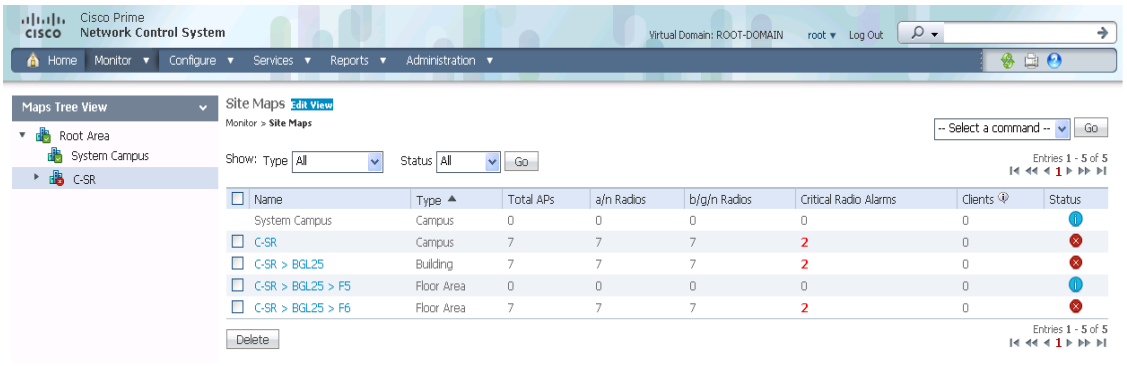
- traffic type active on the network: data or voice traffic or both
- location accuracy requirements
- number of active users
- number of users per square footage

To calculate the recommended number and placement of access points for a given deployment, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

The Site Map page appears (see Figure 4-39).

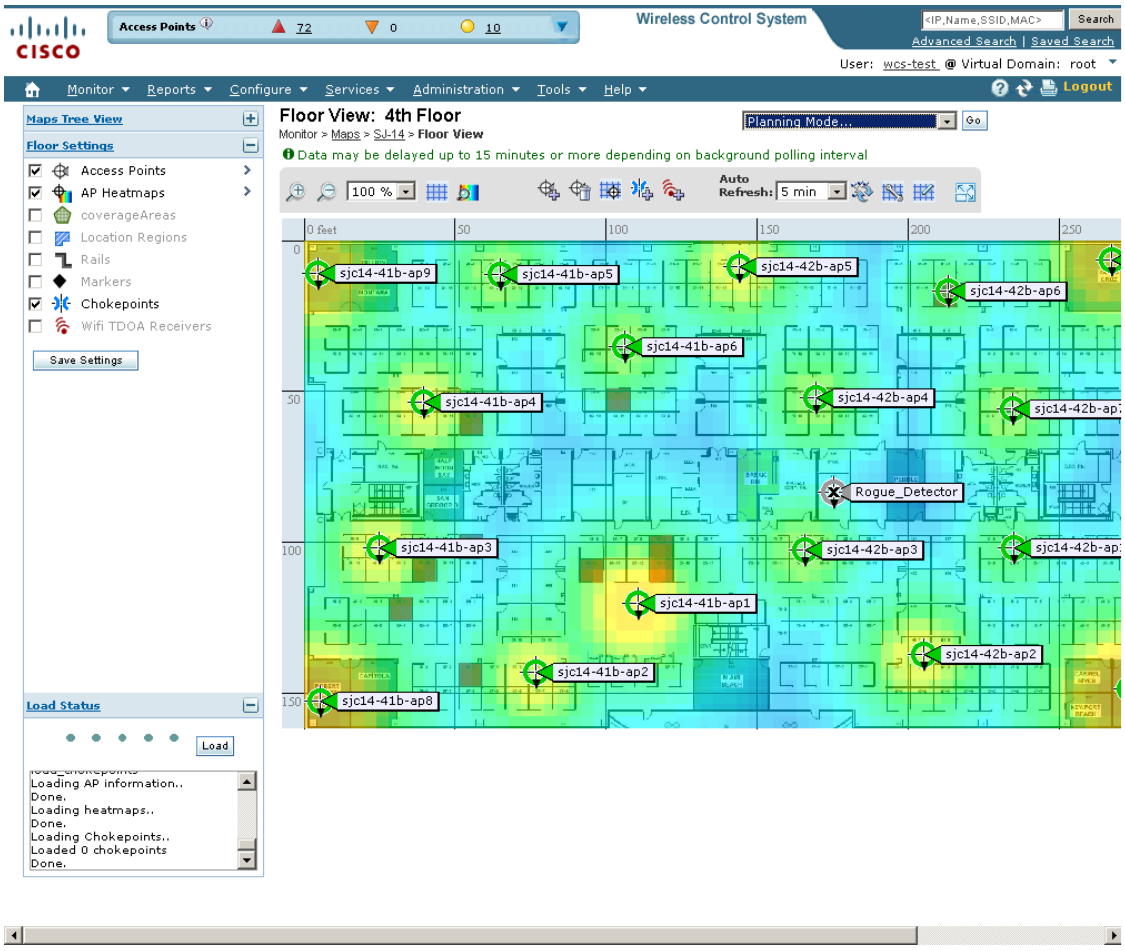
Figure 4-39 Monitor > Site Maps Page



Step 2 Select the appropriate location link from the list that appears.

A color-coded map appears showing placement of all installed elements (access points, clients, tags) and their relative signal strength (see Figure 4-40).

Figure 4-40 Selected Floor Area Showing Current Access Point Assignments



Step 3 Choose **Planning Mode** from the Select a command drop-down list (top-right), and click **Go**. A blank floor map appears.

Step 4 Click **Add APs**.

Step 5 In the page that appears, drag the dashed-line rectangle over the map location for which you want to calculate the recommended access points (see Figure 4-41).

Note Adjust the size or placement of the rectangle by selecting the edge of the rectangle and holding down the **Ctrl** key. Move the mouse as necessary to outline the targeted location.

Figure 4-41 Add APs page

Step 6 Choose **Automatic** from the Add APs drop-down list.

Step 7 Choose the **AP Type** and the appropriate antenna and protocol for that access point.

Step 8 Choose the target throughput for the access point.

Step 9 Select the check box(es) next to the **service(s)** that is used on the floor. Options are Data/Coverage (default), Voice, Location, and Location with Monitor Mode APs. (see Table 4-13).

Note You must select at least one service or an error occurs.

Note If you select the **Advanced Options** check box, two additional access point planning options appear: Demand and Override Coverage per AP. Additionally, a Safety Margin field appears for the Data/Coverage and Voice safety margin options.

Table 4-13 Definition of Services Option

Service Options	Description			
Data/Coverage	Select this check box if data traffic is transmitted on the wireless LAN. The following densities are used depending on the band and data rates:			
	Band	**Path Loss Model (dBm)**	**Date Rate (Mb/s)**	**Area (Sq. ft.)**
	802.11a	–3.3	10-12	6000
	802.11a	–3.3	15-18	4500

Table 4-13 Definition of Services Option (continued)

Service Options	Description			
	802.11a	–3.5	10-12	5000
	802.11a	–3.5	15-18	3250
	802.11bg	–3.3	5	6500
	802.11bg	–3.3	6	4500
	802.11bg	–3.5	5	5500
	802.11bg	–3.5	6	3500
	If you select the **Advanced Options** check box, you can select the desired safety margin (aggressive, safe, or very safe) of the signal strength threshold for data. • Aggressive = Minimum (–3 dBm) • Safe = Medium (0 dBm) • Very Safe = Maximum (+3 dBm)			
Voice	Select the Voice check box, if voice traffic is transmitted on the wireless LAN. If you select the **Advanced Options** check box, you can select the desired safety margin (aggressive, safe, very safe or 7920-enabled) of the signal strength threshold for voice. • Aggressive = Minimum [–78 dBm (802.11a/b/g)] • Safe = Medium [–75 dBm (802.11a/b/g)] • Very Safe = Maximum [(–72 dBm (802.11a/b/g)] • 7920_enabled = [(–72 dBm (802.11a); –67 dBm (802.11b/g)]			
Location	Select this check box to ensure that the recommended access point calculation provides the true location of an element within 10 meters at least 90% of the time. To meet the criteria, access points are collocated within 70 feet of each other in a hexagonal pattern employing staggered and perimeter placement. **Note** Each service option includes all services that are listed above it. For example, if you select the Location check box, the calculation considers data/coverage, voice, and location in determining the optimum number of access points required.			

Table 4-14 Definition of Advanced Services

Service Options	Description			
Data/Coverage	Select this check box, if data traffic is transmitted on the wireless LAN. The following densities are used depending on the band and data rates:			
	Band	**Path Loss Model (dBm)**	**Date Rate (Mb/s)**	**Area (Sq. ft.)**

Table 4-14 Definition of Advanced Services (continued)

Service Options	Description			
	802.11a	–3.3	10-12	6000
	802.11a	–3.3	15-18	4500
	802.11a	–3.5	10-12	5000
	802.11a	–3.5	15-18	3250
	802.11bg	–3.3	5	6500
	802.11bg	–3.3	6	4500
	802.11bg	–3.5	5	5500
	802.11bg	–3.5	6	3500
	If you select the **Advanced Options** check box, you can select the desired safety margin (aggressive, safe, or very safe) of the signal strength threshold for data. • Aggressive = Minimum (–3 dBm) • Safe = Medium (0 dBm) • Very Safe = Maximum (+3 dBm)			
Voice	Select the voice check box, if voice traffic is transmitted on the wireless LAN. If you select the **Advanced Options** check box, you can select the desired safety margin (aggressive, safe, very safe or 7920-enabled) of the signal strength threshold for voice. • Aggressive = Minimum [–78 dBm (802.11a/b/g)] • Safe = Medium [–75 dBm (802.11a/b/g)] • Very Safe = Maximum [(–72 dBm (802.11a/b/g)] 7920_enabled = [(–72 dBm (802.11a); –67 dBm (802.11b/g)]			
Location	Select this check box to ensure that the recommended access point calculation provides the true location of an element within 10 meters at least 90% of the time. To meet the criteria, access points are collocated within 70 feet of each other in a hexagonal pattern employing staggered and perimeter placement. **Note** Each service option includes all services that are listed above it. For example, if you select the Location check box, the calculation considers data/coverage, voice, and location in determining the optimum number of access points required.			
Demand	Select this check box, if you want to use the total number of users or user ratio per access point as a basis for the access point calculation.			

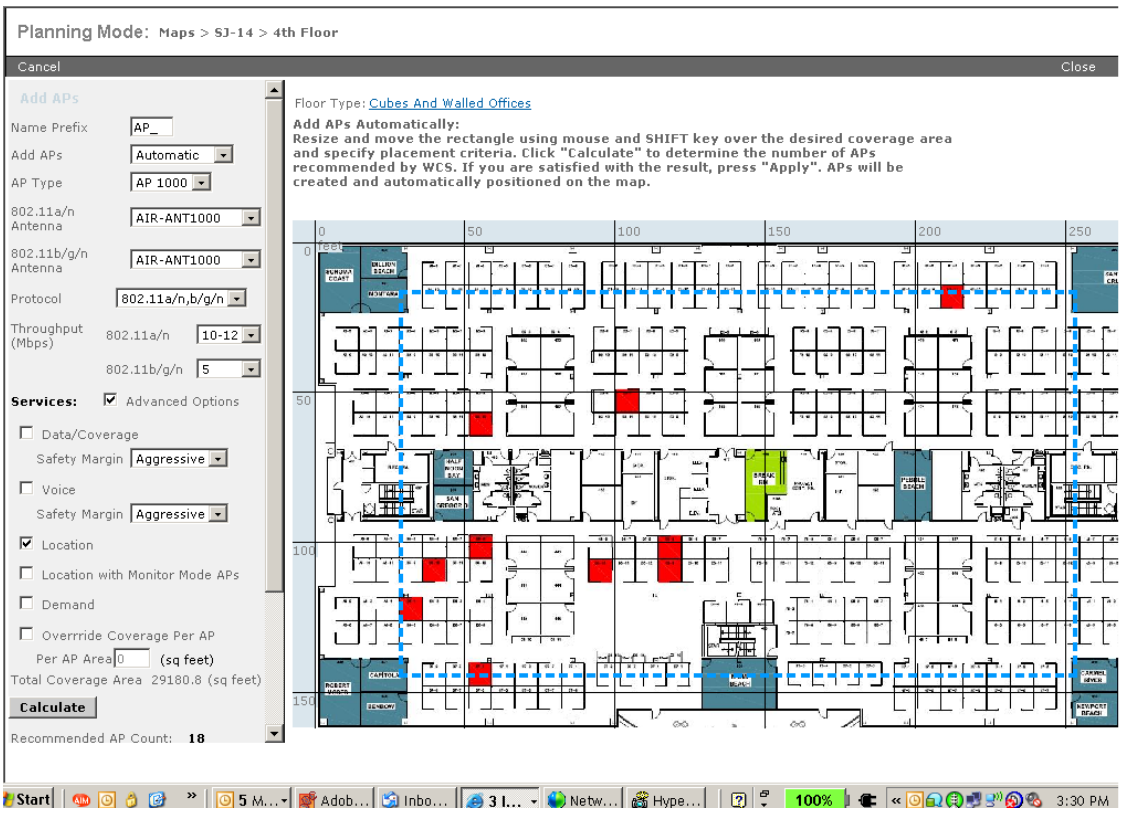
Table 4-14 Definition of Advanced Services (continued)

Service Options	Description
Override Coverage per AP	Select this check box, if you want to specify square foot coverage as the basis for access point coverage.
Safety Margin	Select this check box to qualify relative signal strength requirements for data and voice service in the access point calculation. Options are: Aggressive, Safe, Very Safe, and 7920-enabled (voice only). Select **Aggressive** to require minimal signal strength requirements in the calculation and **Very Safe** to request the highest signal strength.

Step 10 Click **Calculate**.

The recommended number of access points given the selected services appears (see Figure 4-42).

Figure 4-42 Recommended Number of Access Points Given Selected Services and Fields

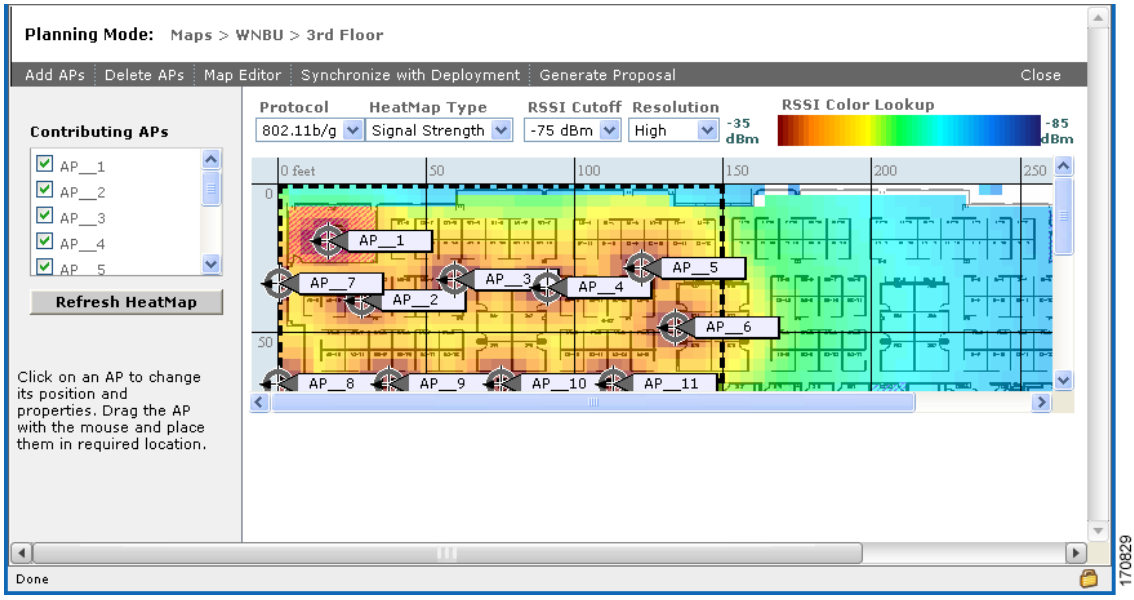


Note Recommended calculations assume the need for consistently strong signals unless adjusted downward by the **safety margin** advanced option. In some cases, the recommended number of access points is higher than what is required.

Note Walls are not used or accounted for in planning mode calculations.

Step 11 Click **Apply** to generate a map that shows proposed deployment of the recommended access points in the selected area based on the selected services and parameters (see Figure 4-43).

Figure 4-43 Recommended Access Point Deployment Given Selected Services and Fields



Step 12 Choose **Generate Proposal** to display a textual and graphical report of the recommended access point number and deployment based on the given input.

Refresh Options

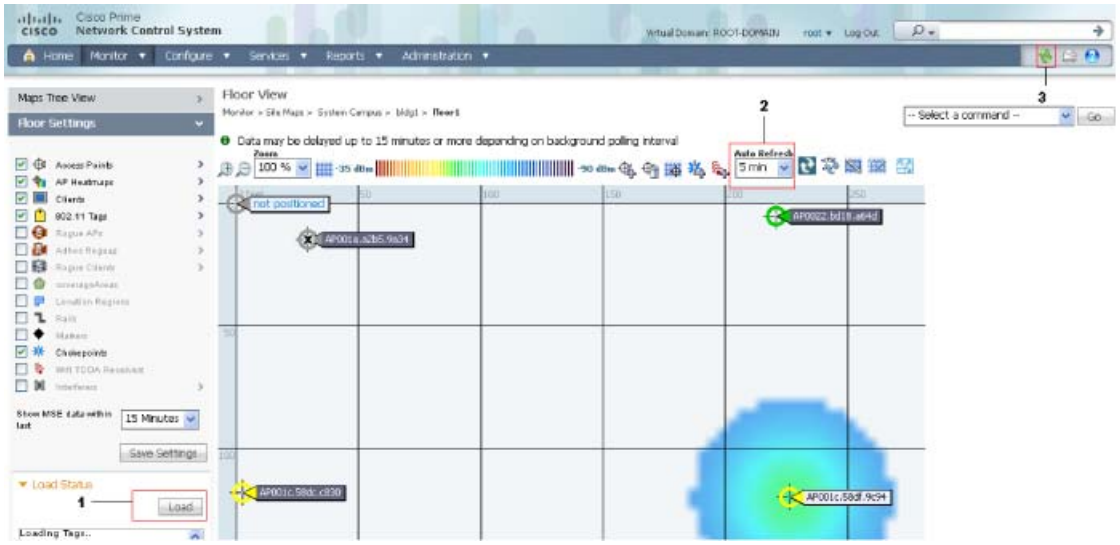
To prepare for monitoring your wireless LANs, become familiar with the various refresh options for a map.

- Load—The Load option in the left sidebar menu refreshes map data from the NCS database on demand (see callout 1 in Figure 4-44).
- Auto Refresh—The Auto Refresh option (see callout 2 in Figure 4-44) provides an interval drop-down list to set how often to refresh the map data from the database.
- Refresh from network—By clicking the **Refresh from network** icon to the right of the Auto Refresh drop-down list (see callout 2 in Figure 4-44), you can refresh the map status and statistics directly from the controller through an SNMP fetch rather than polled data from the NCS database that is five to fifteen minutes older.

Note If you have monitor mode access points on the floor plan, you have a choice between IDS or coverage heatmap types. A coverage heatmap excludes monitor mode access points, and an IDS heatmap includes them.

- Refresh browser—Above the map next to the Logout and Print option is another refresh option (see callout 3 in Figure 4-44). Clicking this refreshes the complete page, or the map and its status and statistics if you are on a map page.

Figure 4-44 Refresh Options



Creating a Network Design

After access points have been installed and have joined a controller, and the NCS has been configured to manage the controllers, set up a network design. A *network design* is a representation within the NCS of the physical placement of access points throughout facilities. A hierarchy of a single campus, the buildings that comprise that campus, and the floors of each building constitute a single network design. These steps assume that the location appliance is set to poll the controllers in that network, as well as be configured to synchronize with that specific network design, to track devices in that environment. The concept and steps to perform synchronization between the NCS and the mobility service engine are explained in the *Cisco 3350 Mobility Services Engine Configuration Guide*.

Designing a Network

To design a network, follow these steps:

Step 1 Open the NCS web interface and log in.

Note To create or edit a network design, you must log into the NCS and have SuperUser, Admin, or ConfigManager access privileges.

Step 2 Choose **Monitor > Site Maps**.

Step 3 From the drop-down list on the right-hand side, choose either New Campus or New Building, depending on the size of the network design and the organization of maps. If you chose New Campus, continue to Step 4. To create a building without a campus, skip to Step 14.

Step 4 Click **Go**.

Step 5 Enter a name for the campus network design, a contact name, and the file path to the campus image file. .bmps and .jpgs are importable.

Note You can use the Browse... button to navigate to the location.

Step 6 Click **Next**.

Step 7 Select the **Maintain Aspect Ratio** check box. Enabling this check box causes the horizontal span of the campus to be 5000 feet and adjusts the vertical span according to the aspect ratio of the image file. Adjusting either the horizontal or vertical span changes the other field in accordance with the image ratio.

You should unselect the Maintain Aspect Ratio check box if you want to override this automatic adjustment. You could then adjust both span values to match the real world campus dimensions.

Step 8 Click **OK**.

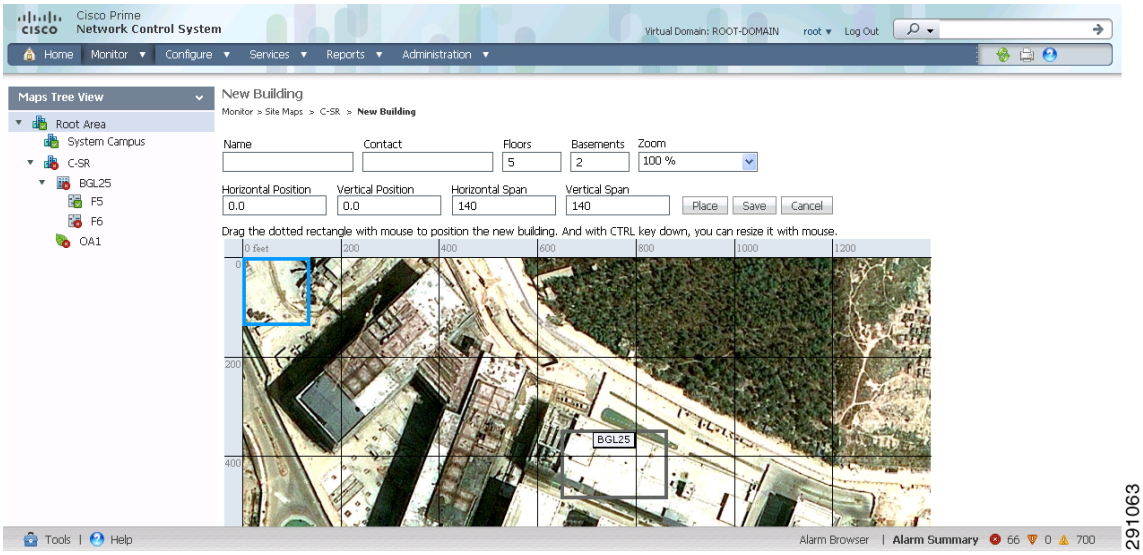
Step 9 In the Monitor > Site Maps page, click the hyperlink associated with the above-made campus map. A page showing the new campus image is displayed.

Step 10 From the Select a command menu on the upper right of the page, choose **New Building**, and click **Go**.

Step 11 Enter the name of the building, the contact person, the number of floors and basements in the building, and the dimensions. Click **OK**.

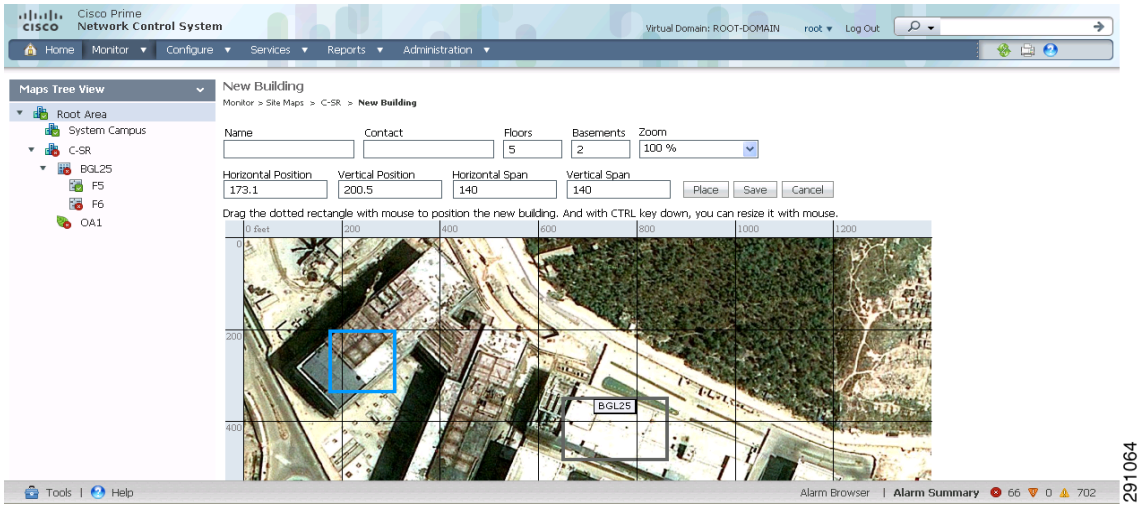
Step 12 Indicate which building on the campus map is the correct building by clicking the blue box in the upper left of the campus image and dragging it to the intended location (see Figure 4-45). To resize the blue box, hold down the **Ctrl** key and click and drag to adjust its horizontal size. You can also enter dimensions of the building by entering numerical values in the Horizontal Span and Vertical Span fields and click **Place**. After resizing, reposition the blue box if necessary by clicking it and dragging it to the desired location. Click **Save**.

Figure 4-45 Repositioning Building Highlighted in Blue



Step 13 The NCS is then returned to the campus image with the newly created building highlighted in a green box. Click the **green box** (see Figure 4-46).

Figure 4-46 Newly Created Building Highlighted in Blue



Step 14 To create a building without a campus, choose **New Building** and click **Go**.

Step 15 Enter the name, contact information, number of floors and basements, and dimension information of the building. Click **Save**. The NCS is returned to the Monitor > Site Maps page.

Step 16 Click the hyperlink associated with the newly created building.

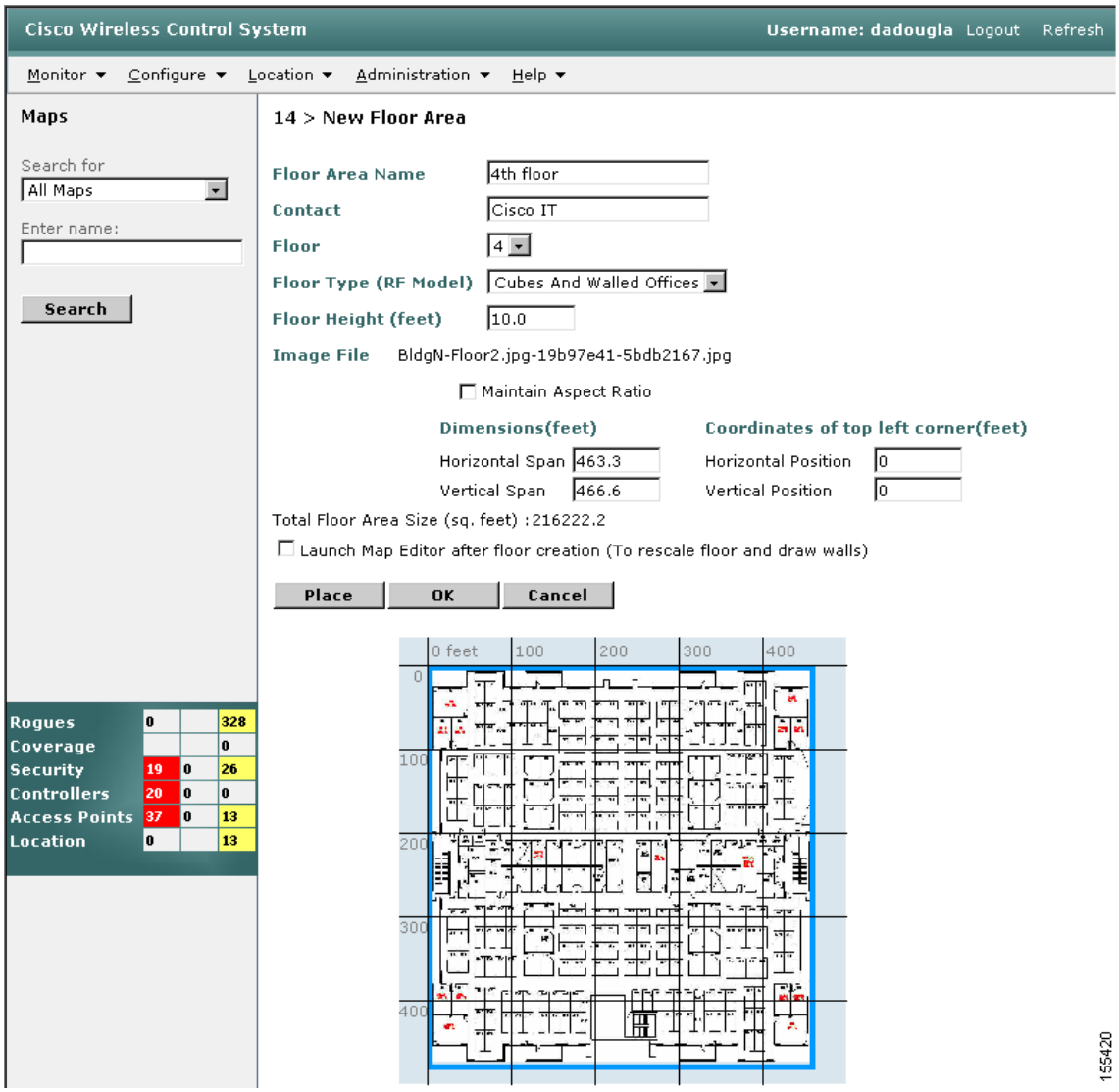
Step 17 In the Monitor > Site Maps > *Campus Name* > *Building Name* page, from the drop-down list and choose **New Floor Area**. Click **Go**.

Step 18 Enter a name for the floor, a contact, a floor number, floor type, and height at which the access points are installed and the path of the floor image. Click **Next**.

Note The Floor Type (RF Model) field specifies the type of environment on that specific floor. This RF Model indicates the amount of RF signal attenuation likely to be present on that floor. If the available models do not properly characterize a floor's makeup, details on how to create RF models specific to a floor's attenuation characteristics are available in the *Cisco 3350 Mobility Services Engine Configuration Guide*.

Step 19 If the floor area is a different dimension than the building, adjust floor dimensions by either making numerical changes to the text fields under the Dimensions heading or by holding the **Ctrl** key and clicking and dragging the blue box around the floor image. If the floor's location is offset from the upper left corner of the building, change the placement of the floor within the building by either clicking and dragging the blue box to the desired location or by altering the numerical values under the **Coordinates of top left corner** heading (see Figure 4-47). After making changes to any numerical values, click Place.

Figure 4-47 Repositioning Using Numerical Value Fields



Step 20 Adjust the characteristics of the floor with the NCS map editor by selecting the check box next to **Launch Map Editor**. For an explanation of the map editor feature, see the "Using the Map Editor" section on page 4-71.

Step 21 At the image of the new floor (Monitor > Site Maps > *CampusName* > *BuildingName* > *FloorName*), go to the drop-down list on the upper right and choose **Add Access Points**. Click **Go**.

Step 22 All access points that are connected to controllers are displayed. Even controllers that the NCS is configured to manage but which have not yet been added to another floor map are displayed. Select the access points to be placed on the specific floor map by checking the boxes to the left of the access point entries. Select the box to the left of the Name column to select all access points. Click **OK**.

Step 23 Each access point you have chosen to add to the floor map is represented by a gray circle (differentiated by access point name or MAC address) and is lined up in the upper left part of the floor map. Drag each access point to the appropriate location. (Access points turn blue when you click them to relocate them.) The small black arrow at the side of each access point represents Side A of each access point, and each arrow of the access point must correspond with the direction in which the access points were installed. (Side A is clearly noted on each 1000 series access point and has no relevance to the 802.11a/n radio.)

Step 24 To adjust the directional arrow, choose the appropriate orientation on the Antenna Angle drop-down list. Click **Save** when you are finished placing and adjusting each direction of the access point.

Note Access point placement and direction must directly reflect the actual access point deployment or the system cannot pinpoint the device location.

Step 25 Repeat these steps to create campuses, buildings, and floors until each device location is properly detailed in a network design.

Importing or Exporting WLSE Map Data

When you convert an access point from autonomous to CAPWAP and from the WLSE to the NCS, one of the conversion steps is to manually re-enter the access point information into the NCS. This can be a time-consuming step. To speed up the process, you can export the information about access points from the WLSE and import it into the NCS.

Note The NCS expects a .tar file and checks for a .tar extension before importing the file. If the file you are trying to import is not a .tar file, the NCS displays an error message and prompts you to import a different file.

To map properties and import a tar file containing WLSE data using the NCS web interface, follow these steps. For more information on the WLSE data export functionality (WLSE version 2.15), see http://<WLSE_IP_ADDRESS>:1741/debug/export/exportSite.jsp.

Step 1 Choose **Monitor > Site Maps**.

Step 2 Choose **Properties** from the Select a command drop-down list, and click **Go**.

Step 3 In the Export/Import AP/LS/SP Placement, click **Browse** to select the file to import.

Step 4 Find and select the .tar file to import and click **Open**.

The NCS displays the name of the file in the Import From field.

Step 5 Click **Import**.

The NCS uploads the file and temporarily saves it into a local directory while it is being processed. If the file contains data that cannot be processed, the NCS prompts you to correct the problem and retry. After the file has been loaded, the NCS displays a report of what is added to the NCS. The report also specifies what cannot be added and why.

If some of the data to be imported already exists, the NCS either uses the existing data in the case of campuses or overwrites the existing data using the imported data in the cases of buildings and floors.

If there are duplicate names between a WLSE site and building combination and an NCS campus (or top-level building) and building combination, the NCS displays a message in the Pre Execute Import Report indicating that it will delete the existing building.

Step 6 Click **Import** to import the WLSE data.

NCS displays a report indicating what was imported.

Note Because a WLSE file has no floor number information, the structure of the floor index calculation after WLSE is imported into the NCS is in descending order. You can click the floor image to go directly to the appropriate floor page.

Step 7 Choose **Monitor > Site Maps** to verify the imported data.

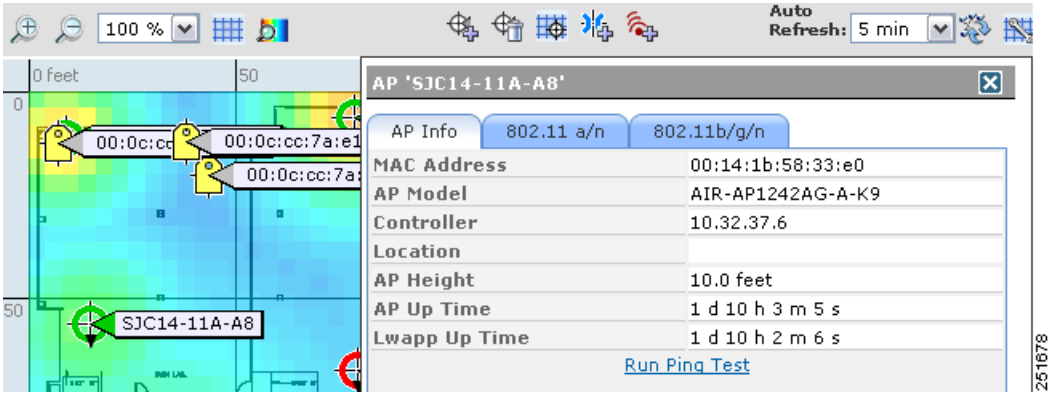
Monitoring Device Details

Access Point Details

Hover your mouse cursor over an access point icon to view access point details (Figure 4-48). Click the appropriate tab to view access point and radio information.

Note Monitor mode access points are shown with gray labels to distinguish them from other access points.

Figure 4-48 Access Point Details



The AP Info tab includes the following access point information:

- MAC address
- Access point model
- Controller
- Location
- Access point height
- Access point uptime
- LWAPP uptime

Note From the AP Info tab, you can run a ping test by clicking the **Run Ping Test** link.

The 802.11 tabs (Figure 4-49) includes the following radio information:

- Channel number
- Extension channel
- Channel width
- Transmit power level
- Client count

Note The number of clients associated to access points might not match the total number of clients.

- Receiving and transmitting utilization percentages
- Channel utilization percentage

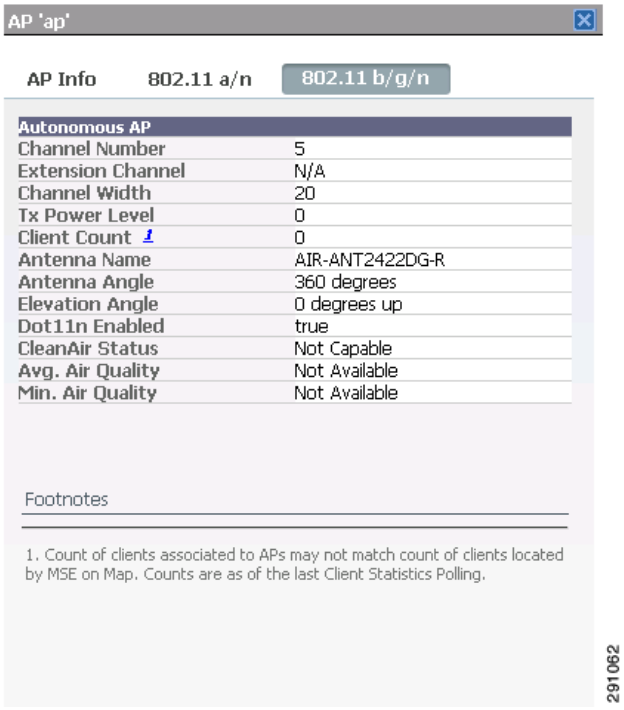
Note Total utilization = (Rx + Tx + Channel utilization) scaled to 100%.

- Antenna name and angle
- Elevation angle

Note From either of the 802.11 tabs, you can view Rx neighbors and radio details for this access point by clicking the appropriate link (**View Rx Neighbors** or **View Radio Details**).

- Dot11n Enabled
- CleanAir Status—Displays the CleanAir status of the access point, whether or not CleanAir is enabled on the access point.
- Average Air Quality—Displays the average air quality on this access point.
- Minimum Air Quality—Displays the minimum air quality on this access point.

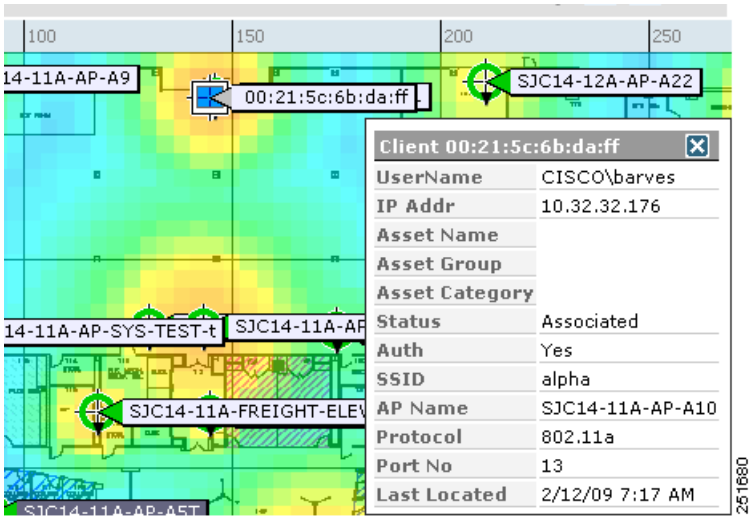
Figure 4-49 802.11 Tabs



Client Details

Hover your mouse cursor over a client icon to view client details (Figure 4-50).

Figure 4-50 Client Details



Client details information includes the following:

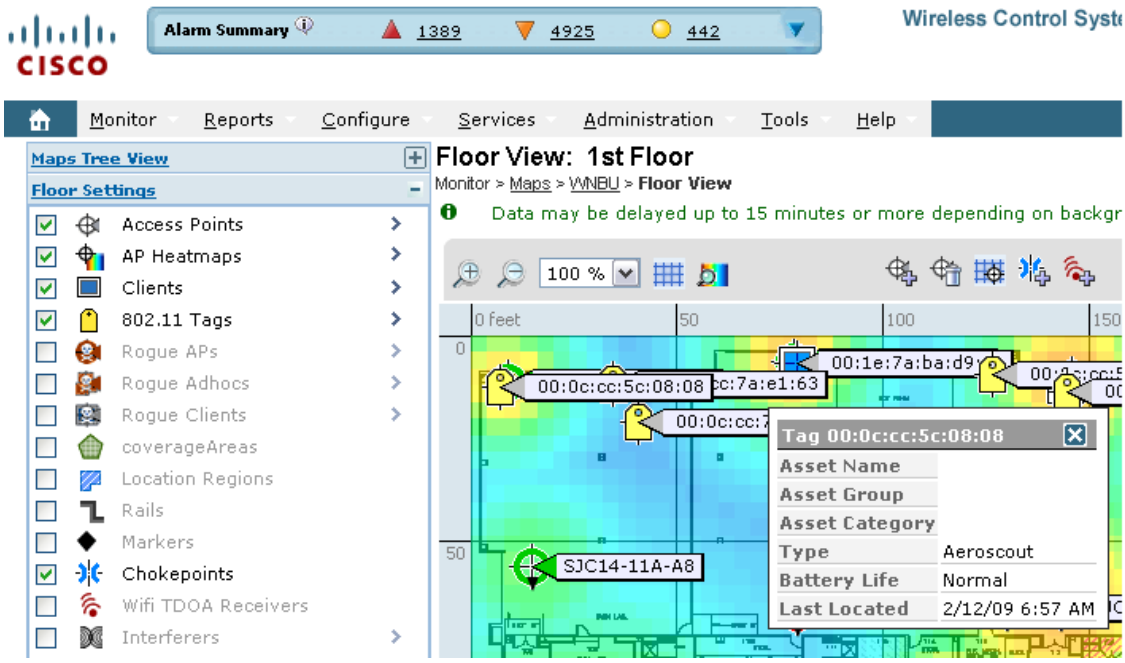
- Username
- IP address

- Asset name, group, and category
- Status
- Auth
- SSID
- Access point name
- Protocol
- Port number
- Last location

Tag Details

Hover your mouse cursor over a tag icon to view tag details (Figure 4-51).

Figure 4-51 Tag Details



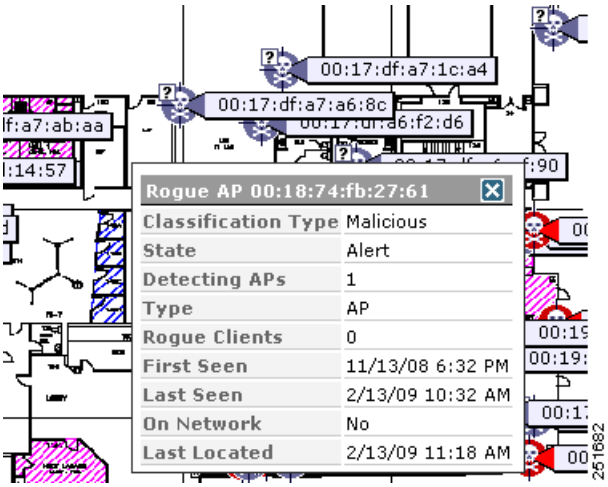
Tag details includes the following:

- Asset name, group, and category
- Type
- Battery life
- Last located

Rogue Access Point Details

Hover your mouse cursor over an access point icon to view rogue access point details (Figure 4-52).

Figure 4-52 Rogue Access Point Details



Rogue access point details includes the following:

- Classification type—Friendly, malicious, or unknown.
- State
- Detecting access points
- Type
- Rogue clients
- First seen
- Last seen
- On network
- Last located

Rogue Adhoc Details

Hover your mouse cursor over an access point icon to view rogue ad hoc details.

Rogue Client Details

Hover your mouse cursor over an access point icon to view rogue client details (Figure 4-53).

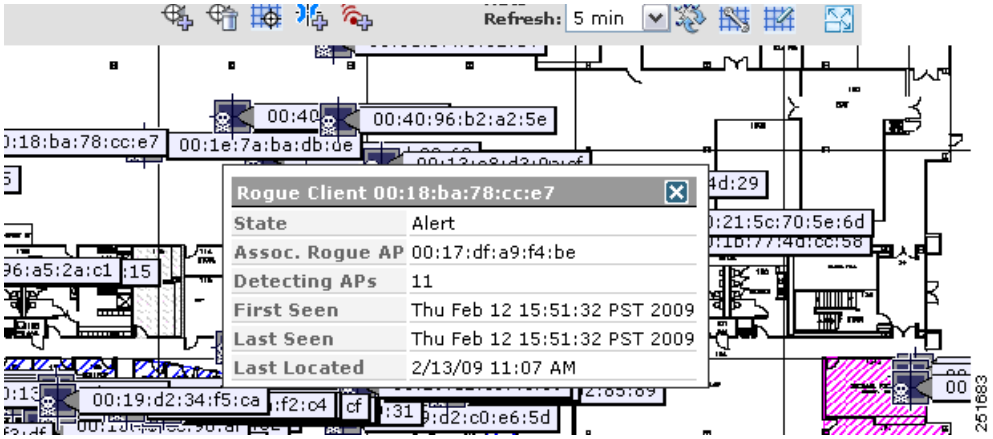
Interferer Details

Hover your mouse cursor over an interferer icon to view its details. Interferer details includes the following:

- Interferer Name—The name of the interfering device.
- Affected Channels—The channel the interfering device is affecting.

- Detected Time—The time at which the interference was detected.
- Severity—The severity index of the interfering device.
- Duty Cycle—The duty cycle (in percentage) of the interfering device.
- RSSI (dBm)—The Received Signal Strength Indicator of the interfering device.

Figure 4-53 Rogue Client Details



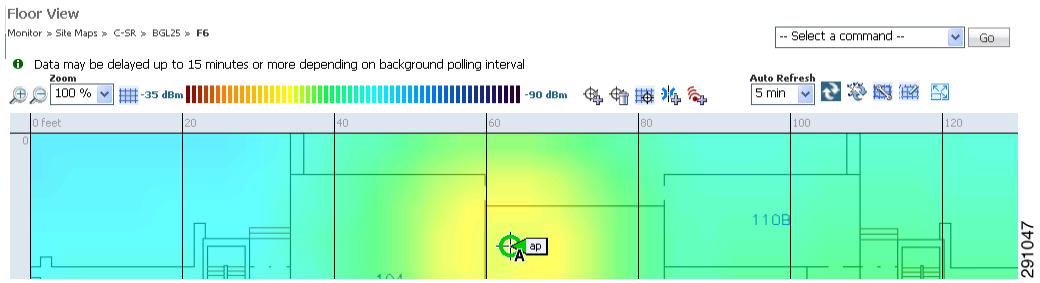
Rogue client details includes the following:

- State
- Associated rogue access point
- Detecting access points
- First seen
- Last seen
- Last located

Floor View Navigation

The main Floor View navigation pane (Figure 4-54) provides access to multiple map functions.

Figure 4-54 Floor View Navigation Pane



This navigation pane includes the following functionality:

- Zoom In/Zoom Out—Click the magnifying glass icon with the plus sign (+) to enlarge the map view. Click the magnifying glass icon with the minus sign (-) to decrease the size of the map view.
- Map Size—Use the map size drop-down list to manually select the map view size (ranging from 50% to 800%).
- Show Grid—Click to show or hide the grid that displays distance in feet on the map.
- RSSI Legend—Hover your mouse cursor over the RSSI Legend icon to display the RSSI color scheme (ranging from red/-35 dBm to dark blue/-90 dBm).
- Add Access Points—Click to open the Add Access Points page. For more information, see the "Adding Access Points to a Floor Area" section on page 4-34.
- Remove Access Points—Click to open the Remove Access Points page. Select the access points that you want to remove and click **OK**. For more information, see "Removing Access Points" section on page 4-39.
- Position Access Points—Click to open the Position Access Points page. For more information, see "Placing Access Points" section on page 4-40.
- Add Chokepoints—Click to open the Add Chokepoints page. For more information, see the *Cisco Context-Aware Services Configuration Guide*.
- Add WiFi TDOA Receivers—Click to open the Add Wi-Fi TDOA Receivers page. For more information, see the *Cisco Context-Aware Services Configuration Guide*.
- Auto Refresh—From the drop-down list, choose the length of time between each system refresh.
- Refresh from Network—Click to initiate an immediate refresh of the current data.
- Planning Mode—Click to open the Planning Mode window. For more information, see the "Using Planning Mode" section on page 4-91 for more information.
- Map Editor—Click to open the Map Editor.

Full Screen—Click to increase the size of the map to full screen. Once there, click **Exit Full Screen** to return to the normal view.

Understanding RF Heatmap Calculation

A radio frequency heat map is a graphical representation of the strength of the RF signals. Because WLANs are very dynamic and nondeterministic in nature, administrators can never be certain of the coverage at a particular moment. To help combat this challenge, the NCS provides a map of your floor plan along with visual cues as to the Wi-Fi coverage of the floor. These maps are called heatmaps because they are similar to the colored maps used to show varying levels of heat in oceanography or geographical sciences. Color is used to show the various levels of signal strength. The different shades in the "heatmap" reflect differing signal strengths.

This color visualization is extremely useful. At one glance, you can see the current state of coverage (without having to walk around measuring it), the signal strength, and any gaps or "holes" in the WLAN. Because floor plans and heat maps are very intuitive, this system greatly enhances the speed and ease with which you support your organization and troubleshoot specific problems.

The RF heatmap calculation is based on an internal grid. Depending on the exact positioning of an obstacle in that grid, the RF heatmap, within a few feet or meters of the obstacle, might or might not account for the obstacle attenuation.

In detail, grid squares partially affected by an obstacle crossing the grid square might or might not incorporate the obstacle attenuation according to the geometry of the access point, obstacle, and grid.

For example, consider a wall crossing one grid square. The midpoint of the grid square is behind the wall from the AP, so the whole grid square is colored with attenuation, including (unfortunately) the top left corner that is actually in front of the wall (see Figure 4-55).

Figure 4-55 Access Point/Grid Example One (Actual Attenuation)

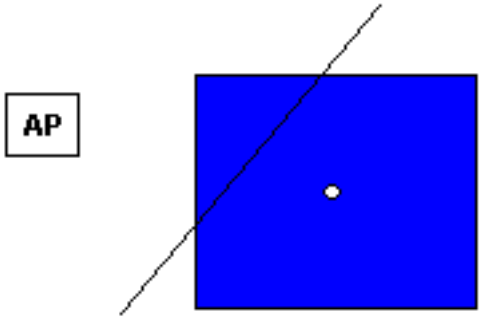
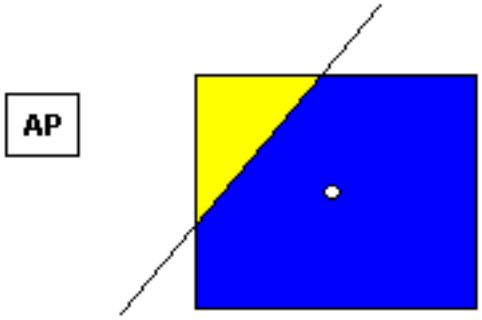


Figure 4-56 displays how the attenuation would ideally appear in this situation.

Figure 4-56 Access Point/Grid Example One (Ideal Attenuation)



The midpoint of the grid square is on the same side of the wall as the AP, so the whole grid square is not colored with attenuation, including (unfortunately) the bottom right corner that is actually behind the wall from the AP (see Figure 4-57).

Figure 4-57 Access Point/Grid Example Two (Actual Attenuation)

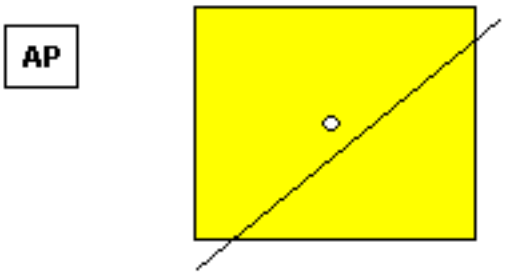
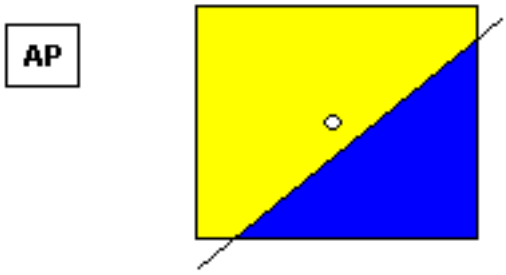


Figure 4-58 displays how the attenuation would ideally appear in this situation.

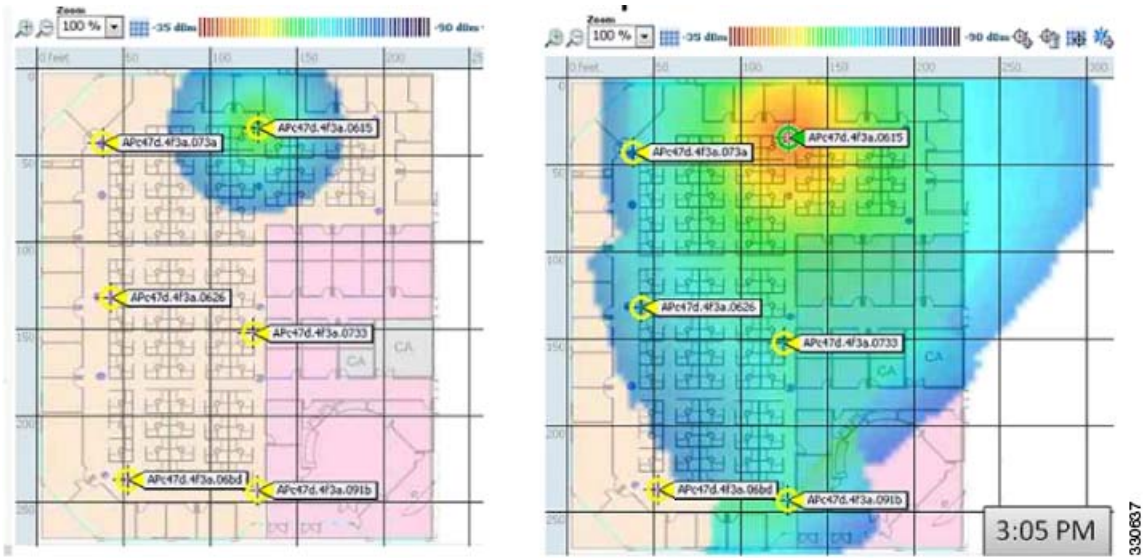
Figure 4-58 Access Point/Grid Example Two (Ideal Attenuation)



Dynamic Heatmap Calculation

The RF heatmap calculation can be static or dynamic. By default it is dynamic, to configure it to be static, disable the dynamic heatmap option in the map properties page.The NCS server maintains the current list of all APs RSSI strength for all APs. The neighbor AP RSSI strength is used to modify the RF heatmaps for all APs. The main purpose of the dynamic heatmap feature is to recompute the RF heatmaps due to obstacles. Figure 4-59 shows the difference between static and dynamic heatmaps.

Figure 4-59 Static Vs Dynamic Heatmap Calculation



Monitoring Google Earth Maps

Within Monitor > Google Earth Maps, you can create an outdoor location, import a file, view Google Earth maps, and specify Google Earth settings.

This section contains the following topics:

Creating an Outdoor Location Using Google Earth

To group the access points together into outdoor locations, use the Latitude/Longitude geographical coordinates for each access point. These coordinates are provided in two ways:

- Importing a KML (Google Keyhole Markup Language) File
- Importing a CSV File (Spreadsheet format with comma-separated values)

This section contains the following topics:

Understanding Geographical Coordinates for Google Earth

The following geographical information is required for each access point:

Note Adding an AP to Google Earth map without having the AP associated on a standard map, you do not see any heatmap when you view the AP in Google Earth.

- Longitude (East or West)—Angular distance in degrees relative to Prime Meridian. Values west of Meridian range from –180 to 0 degrees. Values east of Meridian range from 0 to 180 degrees. The default is 0.

  Coordinates in degrees, minutes, seconds, direction:

  - Degrees (–180 to 180)
  - Minutes (0 to 59)
  - Seconds (00.00 to 59.99)
  - Direction—East or West (E, W)

  Decimal format (converted from degrees, minutes, and seconds):

  - Longitude can range from –179.59.59.99 W to 179.59.59.99 E
- Latitude (North or South)—Angular distance in degrees relative to the Equator. Values south of the Equator range from –90 to 0 degrees. Values north of the Equator range from 0 to 90 degrees. The default is 0.

  Coordinates in degrees, minutes, seconds, direction:

  - Degrees (–90 to 90)
  - Minutes (0 to 59)

  - Seconds (00.00 to 59.99)
  - Direction—North or South (N, S)

  Decimal format (converted from degrees, minutes, and seconds):

  - Latitude can range from –89.59.59.99 S to 89.59.59.99 N

- Altitude—Height or distance of the access point from the surface of the earth in meters. If not provided, value defaults to 0. Values range from 0 to 99999.
- Tilt—Values range from 0 to 90 degrees (cannot be negative). A tilt value of 0 degrees indicates viewing from directly above the access point. A tilt value of 90 degrees indicates viewing along the horizon. Values range from 0 to 90. The default azimuth angle is 0.
- Range—Distance in meters from the point specified by longitude and latitude to the point where the access point is being viewed (the Look At position) (camera range above sea level). Values range from 0 to 999999.
- Heading—Compass direction in degrees. The default is 0 (North). Values range from 0 to ±180 degrees.
- Altitude Mode—Indicates how the <altitude> specified for the Look At point is interpreted.
  - Clamped to ground—Ignores the <altitude> specification and places the Look At position on the ground. This is the default.
  - Relative to ground—Interprets the <altitude> as a value in meters above the ground.
  - Absolute—Interprets the <altitude> as a value in meters above sea level.
- Extend to ground—Indicates whether or not the access point is attached to a mast.

Creating and Importing Coordinates in Google Earth (KML File)

The geographical coordinates can be created in Google Earth and imported. Either a folder or individual placemarks can be created. Creating a folder helps group all the Placemarks into a single folder and allows you to save the folder as a single KML (a.k.a. XML) file. If individual Placemarks are created, each Placemark must be individually saved.

Follow these steps to create a folder in Google Earth:

Step 1 Launch Google Earth.

Step 2 In the Places page on the left sidebar menu, choose **My Places** or **Temporary Places**.

Step 3 Right-click **Temporary Places** and select **Add > Folder** from the drop-down lists.

Note By using a KML file, folders can be created hierarchically to any depth. For example, you can create folders and placemarks organized by country, city, state, zip.
This is not applicable for CSV. In CSV there can be only one level of hierarchy.

Step 4 Enter the following information (optional):

- Name—Folder name
- Description—Folder description
- View—Includes latitude, longitude, range, heading, and tilt

Note If the View coordinates (latitude, longitude, range, heading, and tilt) are specified, this information is used to "fly" or advance to the correct location when Google Earth is first loaded.
If no coordinates are specified, the latitude and longitude information is derived using the minimum and maximum latitude and longitude of all access points within this group or folder.

Step 5 Click **OK** to save the folder. After the folder is created, it can be selected from the Places page to create Placemarks.

To create Placemarks, follow these steps:

Step 1 Launch Google Earth.

Step 2 In the Places page on the left sidebar, select **My Places** or **Temporary Places**.

Step 3 Select the folder that you previously created.

Step 4 Right-click your created folder and select **Add > Placemark** from the drop-down lists.

Step 5 Configure the following parameters, if applicable:

- Name—The Placemark name must contain the name, MAC address, or IP address of the appropriate access point.

  Note The MAC address refers to base radio MAC not Ethernet MAC.

- Latitude—Provides the current coordinate for the folder if the placemark is created inside the folder or the coordinate for the placemark (if not created inside a folder). This field is automatically filled depending on where the yellow Placemark icon is located on the map. Use your mouse to move the Placemark to the correct location or enter the correct coordinate in the Latitude text box.
- Longitude—Provides the current coordinate for the folder if the placemark is created inside the folder or the coordinate for the placemark (if not created inside a folder). This field is automatically filled depending on where the yellow Placemark icon is located on the map. Use your mouse to move the Placemark to the correct location or enter the correct coordinate in the Longitude text box.
- Description (optional)—Field is ignored by the NCS.
- Style, Color (optional)—Field is ignored by the NCS.
- View—Allows you to configure the Latitude, Longitude, Range, Heading and Tilt coordinates. See the "Understanding Geographical Coordinates for Google Earth" section on page 4-113" for more information on these geographical coordinates.
  - Longitude and latitude are automatically filled depending on where the yellow Placemark icon is located on the map. Use your mouse to click and move the Placemark to the correct location.
  - All of the coordinates can be entered manually.
- Altitude—Enter the altitude in meters in the text box or use the Ground to Space slide bar to indicate the altitude.
  - Clamped to ground—Indicates that the Look At position is on the ground. This is the default.
  - Relative to ground—Interprets the <altitude> as a value in meters above the ground.

- Absolute—Interprets the <altitude> as a value in meters above sea level.
- Extend to ground—For Relative to ground or Absolute settings, indicates whether or not the access point is attached to a mast.

Step 6 When all coordinates are entered, click **Snapshot current view** or click **Reset** to return the coordinates to the original settings.

Note For more information regarding Google Earth, see to the Google Earth online help.

Step 7 Click **OK**.

Step 8 Repeat these steps for all placemarks you want to add.

Step 9 When all placemarks are created, save the folder as a .kmz file (KML Zip file) or as a .kml file.

Note A .kmz file should contain only one .kml file.

Note To save the folder, right-click the folder, select **Save as** from the drop-down list, navigate to the correct location on your computer, and click **Save**. Both .kmz and .kml files can be imported into the NCS.

Creating and Importing Coordinates as a CSV File

To create a CSV file to import into the NCS, follow these steps:

Step 1 Open a flat file and provide the necessary information as a comma-separated list. The Table 4-15 lists the potential data, whether the data is optional or required, and the parameters of the data.

Note For more information regarding the geographical coordinates listed in Table 4-15, see the "Understanding Geographical Coordinates for Google Earth" section on page 4-113.

Table 4-15 Potential Fields for the CSV File

"FolderName"	"Value Optional"	Max Length: 32
"FolderState"	"Value Optional"	Permitted Values: true/false
"FolderLongitude"	"Value Optional"	Range: 0 to ±180
"FolderLatitude"	"Value Optional"	Range: 0 to ±90
"FolderAltitude"	"Value Optional"	Range: 0 to 99999
"FolderRange"	"Value Optional"	Range: 0 to 99999
"FolderTilt"	"Value Optional"	Range: 0 to 90
"FolderHeading"	"Value Optional"	Range: 0 to ±180
"FolderGeoAddress"	"Value Optional"	Max Length: 128

Table 4-15 Potential Fields for the CSV File (continued)

"FolderName"	"Value Optional"	Max Length: 32
"FolderGeoCity"	"Value Optional"	Max Length: 64
"FolderGeoState"	"Value Optional"	Max Length: 40
"FolderGeoZip"	"Value Optional"	Max Length: 12
"FolderGeoCountry"	"Value Optional"	Max Length: 64
"AP_Name"	"Value Required"	Max Length: 32
"AP_Longitude"	"Value Required"	Range: 0 to ±180
"AP_Latitude"	"Value Required"	Range: 0 to ±90

Step 2 Save the .csv file. The file is now ready to import into the NCS.

Importing a File into NCS

To import a Google KML or a CSV into the Google Earth Maps feature of the NCS, follow these steps:

Step 1 Log in to the NCS.

Step 2 Choose **Monitor > Google Earth Maps**.

Step 3 From the Select a command drop-down list, choose **Import Google KML** or **Import CSV**.

Step 4 Click **Go**.

Step 5 Use the Browse button to navigate to the .kml, .kmz, or .csv file on your computer.

Step 6 When the file name path is displayed in the text box, click **Next**.

The input file is parsed and validated for the following:

- Access points specified in the uploaded file are validated (the specified access points must be available within the NCS).
- Range validations are performed for tilt, heading, range, and other geographical coordinates fields.If longitude and latitudeare provided, range validations are performed; if not, the value is defaulted to 0.

Note In KML, the longitude and latitude ranges can only be entered in decimal format. In CSV, different formats are supported (see the CSV sample under Google Maps > Import CSV).

Note If the input file does not validate for completeness, an error page appears. The uploaded information cannot be saved until all errors are corrected.

Step 7 After the files pass all validation checks, review the file details and click **Save**.

If the uploaded information was saved previously, the information is overwritten accordingly:

- If the folder was uploaded previously, the coordinates are updated for the folder.

- If access points were uploaded previously, the coordinates are updated for the access points.
- Existing access points in the folder are not removed.
- New folders, as needed, are created and access points are placed accordingly.

Viewing Google Earth Maps

To view Google Earth maps, follow these steps:

Step 1 Log in to the NCS.

Step 2 Choose **Monitor > Google Earth Maps**. The Google Earth Maps page displays all folders and the number of access points included within each folder.

Step 3 Click **Launch** for the map you want to view. Google Earth opens in a separate page and displays the location and its access points.

Note To use this feature, you must have Google Earth installed on your computer and configured to auto-launch when data is sent from the server. You can download Google Earth from the Google website: http://www.google.com/earth/index.html.

Viewing Google Earth Map Details

To view details for a Google Earth Map folder, follow these steps:

Step 1 In the Google Earth Map page, click the folder name to open the details page for this folder. The Google Earth Details provide the access point names and MAC or IP addresses.

Note To delete an access point, select the applicable check box and click **Delete**.
To delete the entire folder, select the check box next to **Folder Name** and click **Delete**. Deleting a folder also deletes all subfolders and access points inside the folder.

Step 2 Click **Cancel** to close the details page.

Adding Google Earth Location Launch Points to Access Point Pages

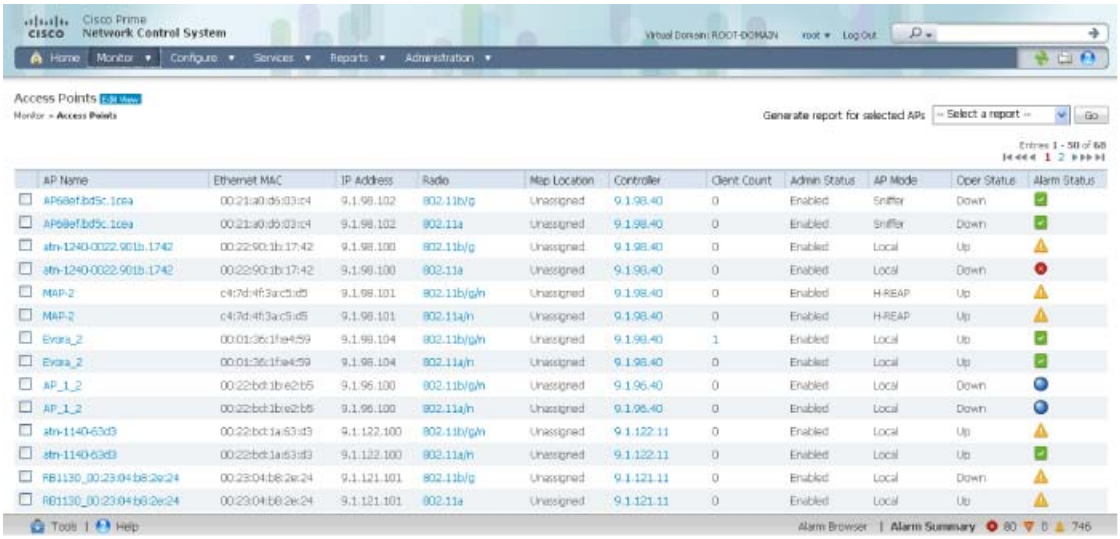
You can expand the number of Google Earth Location launch points within the NCS by adding it to the Access Point summary and detail pages.

To add a Google Earth Location launch point to the Access Point summary and details page, follow these steps:

Step 1 Choose **Monitor > Access Points** (see Figure 4-60).

Step 2 In the Access Point summary page, click the **Edit View** link next to page heading.

Figure 4-60 Monitor > Access Points Page



Step 3 In the Edit View page, highlight **Google Earth Location** in the left-hand column. Click **Show**.

The Google Earth Location column heading moves into the View Information column.

Note The View Information listings, top-to-bottom, reflect the left-to-right order of the columns as they appear on the Access Point summary page.

Step 4 To change the display order of the columns, highlight the Google Earth Location entry and click the **Up** and **Down** buttons as needed. Click **Submit**.

You are returned to the Access Points summary page, and a Google Earth launch link is in the display.

Note The launch link also appears in the general summary page of the Access Points details page (Monitor > Access Points > *AP Name)*.

Google Earth Settings

Access point related settings can be defined from the Google Earth Settings page. To configure access point settings for the Google Earth Maps feature, follow these steps:

Step 1 Choose **Monitor > Google Earth Maps**.

Step 2 Configure the following parameters:

- Refresh Settings—Select the **Refresh from Network** check box to enable this on-demand refresh. This option is applied only once and then disabled.

Caution Because this refresh occurs directly from the network, it could take a long period of time to collect data according to the number of access points.

- Layers—Layer filters for access points, access point heat maps, and access point mesh information can be selected and saved. Select the check box to activate the applicable layer and click **>** to open the filter page.

  Note These settings apply when Google Earth sends the request for the next refresh.

  - Access Points—From the AP Filter drop-down list, choose to display channels, Tx power level, coverage holes, MAC addresses, names, controller IP, utilization, profiles, or clients.

    Note If the access point layer is not checked, no data is returned, and an error message is returned to Google Earth as a Placemark without an icon.

  - AP Heatmap—From the Protocol drop-down list, choose 802.11a/n, 802.11b/g/n, 802.11a/n & 802.11b/g/n, or None. Select the cutoff from the RSSI Cutoff drop-down list (- 60 to - 90 dBm).

    Note If the protocol chosen is both 802.11a/n and 802.11b/g/n, the heat maps are generated for both and overlaid on top of each other. The order cannot be defined. To prevent this overlay, you must turn off individual overlay in Google Earth or change it in the Google Earth Settings on the NCS.

  - AP Mesh Info—Choose Link SNR, Packet Error Rate, or none from the Link Label drop-down list. Choose Link SNR or Packet Error Rate from the Link Color drop-down list.

    Note When the AP Mesh Info check box is chosen, Mesh Links are also automatically shown.

Step 3 Click **Save Settings** to confirm these changes or **Cancel** to close the page without saving the changes.

CHAPTER 6

Managing NCS User Accounts

The Cisco NCS Administration enables you to schedule tasks, administer accounts, and configure local and external authentication and authorization. Also, set logging options, configure mail servers, and data management related to configuring the data retain periods. Information is available about the types of NCS licenses and how to install a license.

Organizations need an easy and cost-effective method to manage and control wireless network segments using a single management platform. They need a solution that supports limiting an individual administrator to manage or control the wireless LAN.

This chapter describes the administrative tasks to perform with NCS. It contains the following sections:

Managing NCS User Accounts

This section describes how to configure global e-mail parameters and manage NCS user accounts. It contains the following topics:

Adding NCS User Accounts

This section describes how to configure a NCS user. The accounting portion of the AAA framework is not implemented at this time. Besides complete access, you can give administrative access with differentiated privileges to certain user groups. NCS supports external user authentication using these access restrictions and authenticates the users against the TACACS+ and RADIUS servers.

The username and password supplied by you at install time are always authenticated, but the steps you take here create additional superusers. If the password is lost or forgotten, you must run a utility to reset the password to another user-defined password.

To add a new user account to NCS, follow these steps:

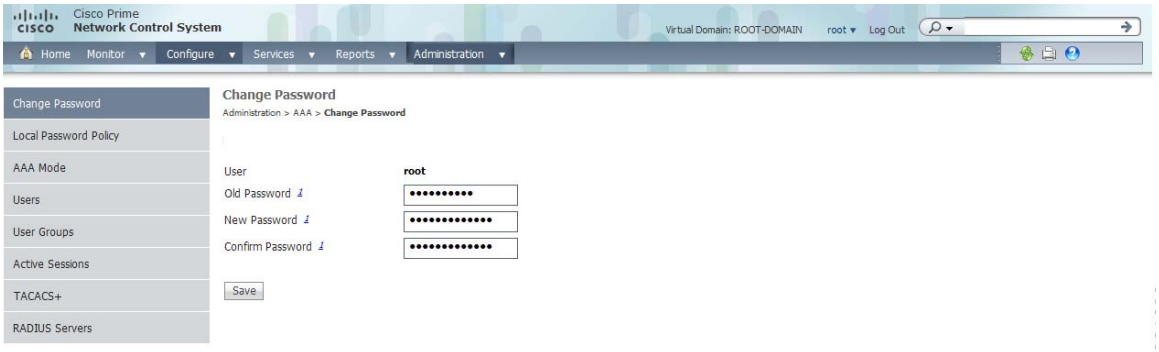
Step 1 Start the NCS server by following the instructions in the "Starting the NCS Server" section on page 2-10.

Step 2 Log into the NCS user interface as *root*.

Note We recommend that you create a new superuser assigned to the SuperUsers group.

Step 3 Choose **Administration > AAA**. The Change Password page appears (see Figure 6-1).

Figure 6-1 Change Password Page



Step 4 In the Old Password text box, enter the current password that you want to change.

Step 5 Enter the username and password for the new NCS user account. You must enter the password twice.

Note These entries are case sensitive.

Step 6 Choose **User Groups** from the left sidebar menu. The All Groups page displays the following group names (see Figure 6-4).

Note Some usergroups cannot be combined with other usergroups. For instance, you cannot choose both lobby ambassador and monitor lite.

- System Monitoring—Allows users to monitor NCS operations.
- ConfigManagers—Allows users to monitor and configure NCS operations.

- Admin—Allows users to monitor and configure NCS operations and perform all system administration tasks.

Note If you choose admin account and log in as such on the controller, you can also see the guest users under Local Net Admin.

- SuperUsers—Allows users to monitor and configure NCS operations and perform all system administration tasks including administering NCS user accounts and passwords. Superusers tasks can be changed.
- Users Assistant—Allows only local net user administration. User assistants cannot configure or monitor controllers. They must access the Configure > Controller page to configure these local net features.

Note If you create a user assistant user, log in as that user, and choose **Monitor > Controller**, you receive a "permission denied" message, which is an expected behavior.

- Lobby Ambassador—Allows access for configuration and management of only Guest User user accounts.
- Monitor lite—Allows monitoring of assets location.
- Root—Allows users to monitor and configure NCS operations and perform all system administration tasks including changing any passwords. Only one user can be assigned to this group and is determined upon installation. It cannot be removed from the system, and no task changes can be made for this user.

Step 7 Click the name of the user group to which you assigned the new user account. The Group Detail > *User Group* page shows a list of this permitted operations of the group.

From this page you can also show an audit trail of login and logout patterns or export a task list.

Step 8 Make any desired changes by selecting or unselecting the appropriate check boxes for task permissions and members.

Note Any changes you make affect all members of this user group.

Note To view complete details in the Monitor > Client details page and to perform operations such as Radio Measurement, users in User Defined groups need permission for Monitor Clients, View Alerts & Events, Configure Controllers, and Client Location.

Step 9 Click **Submit** to save your changes or **Cancel** to leave the settings unchanged.

Deleting NCS User Accounts

To delete a NCS user account, follow these steps:

Step 1 Start NCS server by following the instructions in the "Starting the NCS Server" section on page 2-10.

Step 2 Log into the NCS user interface as a user assigned to the SuperUsers group.

Step 3 Choose **Administration > AAA**.

Step 4 Choose **Users** from the left sidebar menu to display the Users page.

Step 5 Select the check box to the left of the user account(s) to be deleted.

Step 6 From the Select a command drop-down list, choose **Delete User(s)**, and click **Go**.

When prompted, click **OK** to confirm your decision. The user account is deleted and can no longer be used.

Changing Passwords

To change the password for a NCS user account, follow these steps:

Step 1 Start NCS server by following the instructions in the "Starting the NCS Server" section on page 2-10.

Step 2 Log into the NCS user interface as a user assigned to the SuperUsers group.

Step 3 Choose **Administration > AAA** to display the Change Password page.

Step 4 Enter your old password.

Step 5 Enter the new password in both the New Password and Confirm New Password text boxes.

Step 6 Click **Save** to save your changes. The password for this user account has been changed and can be used immediately.

Changing the Root User Password using CLI

To change the password for a root user using the command-line interface, follow these steps:

Step 1 Log into the system as administrator.

Step 2 Using the command-line interface (CLI), enter the following commands:

```
VMNCS/admin# ncs password ?
  ftpuser  Modifies ftp username and password
  root     Modifies root user login password

VMNCS/admin# ncs password root ?
  password  Modifies root user login password

VMNCS/admin# ncs password root password ? <password>
  <WORD>  Type in root user login password (Max Size - 80)
```

Monitoring Active Sessions

To view a list of active users, follow the steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Active Sessions**. The Active Sessions page appears.

The user highlighted in red represents your current login. If a column heading is a hyperlink, click the heading to sort the list of active sessions in descending or ascending order along that column. The sort direction is toggled each time the hyperlink is clicked.

The Active Sessions page has the following columns:

- Username—The logged in username.
- IP/Host Name—The IP address or the hostname of the machine on which the browser is running. If the hostname of the user machine is not in DNS, the IP address is displayed.
- Login Time—The time at which the user logged in to NCS. All times are based on the NCS server machine time.
- Last Access Time—The time at which the user last accessed NCS. All times are based on the NCS server machine time.

Note The time displayed in this column is usually a few seconds behind the current system time because Last Access Time is updated frequently by the updates to the alarm status dashlet.

- Login Method:
  - Regular: Sessions created for users who log into NCS directly through a browser.
- User Groups: The list of groups to which the user belongs.
- Audit trail icon: Link to page that displays the audit trail (previous login times) for that user.

Viewing or Editing User Account Information

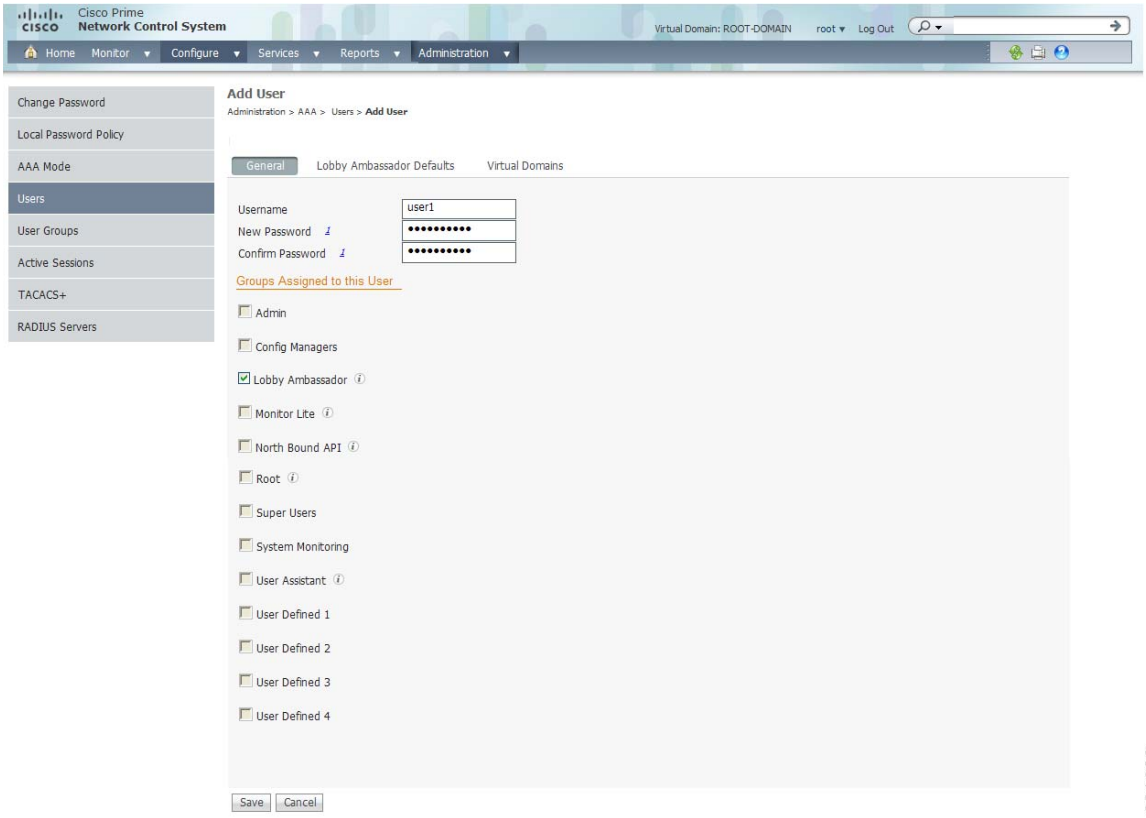
To see the group the user is assigned to or to adjust a password or group assignment for that user, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 Click a user in the User Name column. The User Detail : *User Group* page appears (see Figure 6-2).

Figure 6-2 Detailed Users Page



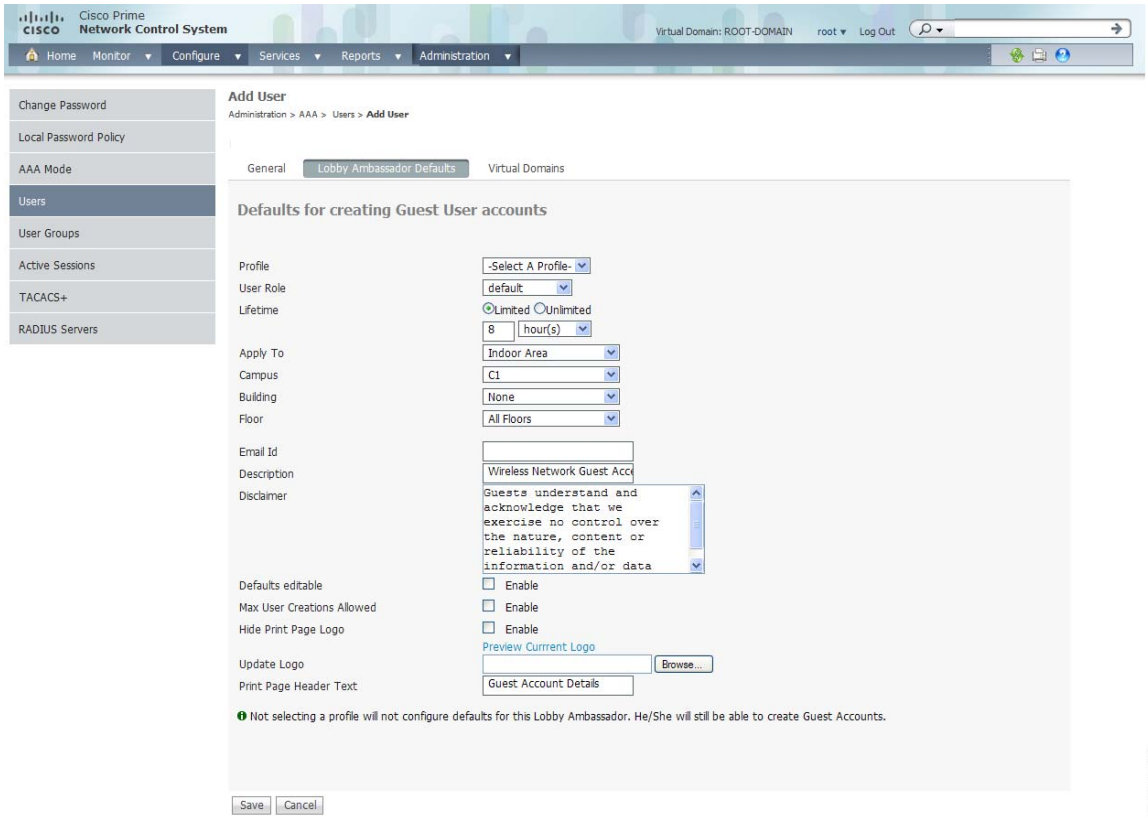
You can see which group is assigned to this user or change a password or group assignment.

Setting the Lobby Ambassador Defaults

If you choose a Lobby Ambassador from the User Name column, a Lobby Ambassador Defaults tab appears (see Figure 6-3). All of the guest user accounts created by the lobby ambassador have these credentials by default. If the default values are not specified, the lobby ambassador must provide the required guest user credential fields.

Note If no default profile is chosen on this tab, the defaults do not get applied to this lobby ambassador. The lobby ambassador account does get created, and you can create users with any credentials you choose.

Figure 6-3 Lobby Ambassador Default Tab



Step 1 Use the Profile drop-down list to choose the guest user to connect to.

Wired-guest is an example of a profile that might be defined to indicate traffic that is originating from wired LAN ports. See the "Configuring Wired Guest Access" section on page 8-47.

Step 2 Choose a user role to manage the amount of bandwidth allocated to specific users within the network. They are predefined by the administrator and are associated with the guests' access (such as contractor, customer, partner, vendor, visitor, and so on).

Step 3 Choose **Limited** or **Unlimited** at the Lifetime radio button.

- For the limited option, you choose the period of time that the guest user account is active using the hours and minutes drop-down lists. The default value for Limited is one day (8 hours).
- When *unlimited* is chosen, no expiration date for the guest account exists.

Step 4 Use the Apply to drop-down list to choose from the following options. What you choose determines what additional parameters appear.

- Indoor area—A campus, building, or floor.
- Outdoor area—A campus or outdoor area.
- Controller list—A list of controller(s) with the selected profile created.
- Config Group—Those config group names configured on NCS.

Step 5 Enter the e-mail ID of the host to whom the guest account credentials are sent.

Step 6 Provide a brief description of the account.

Step 7 If you want to supply disclaimer text, enter it.

Select the **Defaults Editable** check box if you want to allow the lobby ambassador to override these configured defaults. This allows the Lobby Ambassadors to modify Guest User default settings while creating guest account from the Lobby Ambassador portal.

Note If no default profile is selected on this tab, the defaults are not applied to this Lobby Ambassador. However, the Lobby Ambassador account is created, and the Lobby Ambassador can create users with credentials as desired.

Step 8 Select the **Max User Creations Allowed** check box to set limits on the number of guest users that can be created by the lobby ambassador in a given time period. The time period is defined in hours, days, or weeks.

Step 9 Click the **Preview Current Logo** link to see what is currently being used as a logo, and then you can click to enable it or browse to another location to update the logo.

Step 10 If you want additional page header text, you can enter it at the Print Page Header Text field.

Step 11 Click **Submit**.

Viewing or Editing Group Information

To see specific tasks the user is permitted to do within the defined group or make changes to the tasks, follow these steps:

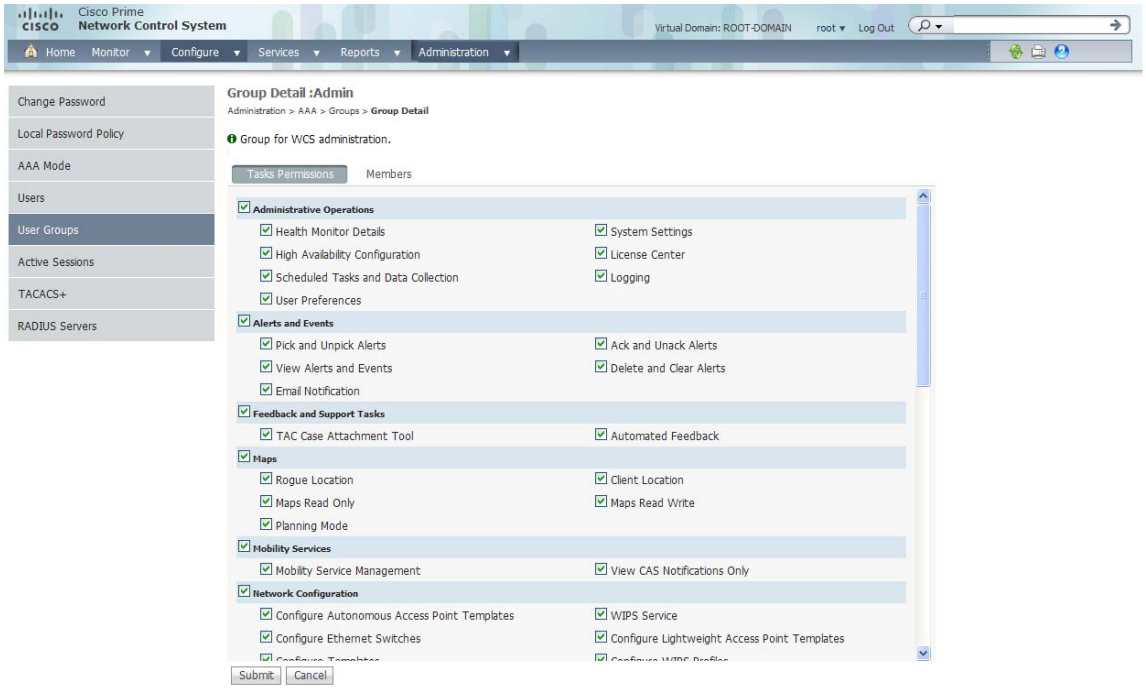
Step 1 Choose **Administration > AAA**.

Step 2 Choose **Users** from the left sidebar menu.

Step 3 Click the group link in the **Member Of** column. The Group Detail: *User Group* page appears (see Figure 6-4).

Note The detailed page varies based on what group you choose (see Figure 6-4).

Figure 6-4 Detailed Group Page



You can see the specific tasks the user is permitted to do within the defined group or make changes to the tasks.

Editing the Guest User Credentials

Click the NCS username of the guest user whose credentials you want to edit. The Lobby Ambassador Default tab appears, and you can modify the credentials.

Note While editing, if the *Profile* selection is removed (changed to *Select a profile*), the defaults are removed for this Lobby Ambassador. The user must reconfigure the defaults to reinforce them.

Viewing the Audit Trail

Click the icon in the Users page to view the configuration changes performed by individual users. The Audit Trail page appears.

This page enables you to view the following data:

- User—User login name.
- Operation—Type of operation audited.
- Time—Time operation was audited.
- Status—Success or failure.

- Reason—Indicates any login failure reason, for example, invalid password.
- Configuration Changes—This field provides a Details link if there are any configuration changes. Click the **Details** link for more information on the configuration changes done by an individual user. The entries list the change of values for individual parameters between NCS and Controller. For more information on Audit Trail Details, see "Audit Trail Details Page" section on page 6-10.

Note The audit trail entries could be logged for individual controller changes. For example, If a template is applied on multiple controllers, then there are multiple audit entries for each controller to which the template has been applied to.

Audit Trail Details Page

The Configuration Changes column in the Audit Trail list page contains a Details link if there are changes to the configuration. Click the **Details** link to view the Audit Trail Details for a specific User. The Audit Trail Details dialog box shows the attribute-level differences when a User changes the configuration from either the Templates or Configuration side.

Table 6-1 describes the fields in the Audit Trail Details dialog box.

Fields	Description
NCS Username	The username who triggered this audit trail.
Object Name	The name of the object that has triggered this audit trail.
Operation Time	The date and time at which the audit entry was made.
Configuration Changes	Lists the attributes that have been changed as a result of a user action in NCS and the controller. For example, the attributes could be: • Quality of service • Admin Status • MAC Filters

Creating Guest User Accounts

You can use the Cisco Lobby Ambassador to create guest user accounts in NCS. A guest network provided by an enterprise allows access to the Internet for a guest without compromising the host. The web authentication is provided with or without a supplicant or client, so a guest needs to initiate a VPN tunnel to their desired destinations.

Both wired and wireless guest user access is supported. Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

The network administrator must first set up a lobby ambassador account. Guest user accounts are for visitors, temporary workers, and so on. who need network access. A lobby ambassador account has limited configuration privileges and only allows access to the screens used to configure and manage guest user accounts.

The lobby ambassador can create the following types of guest user accounts:

- A guest user account with a limited lifetime. After the specified time period, the guest user account automatically expires.
- A guest user account with an unlimited lifetime. This account never expires.
- A guest user account that is activated at a predefined time in the future. The lobby ambassador defines the beginning and end of the valid time period.

To create guest user accounts in NCS, follow these steps:

Note A group that has the SuperUser/administrator privileges (by default) can create a lobby ambassador account. Multiple lobby ambassador accounts can be created by the administrator with varying profiles and permissions.

Note A root group, which is created during installation, has only one assigned user, and no additional users can be assigned after installation. This root user cannot be changed. Also, unlike a super user, no task changes are allowed.

Step 1 Log into the NCS user interface as an administrator.

Step 2 Choose **Administration > AAA**.

Step 3 From the left sidebar menu, choose **Users**.

Step 4 From the Select a command drop-down list, choose **Add User**, and click **Go**. The Users page appears.

Step 5 Enter the username.

Step 6 Enter the password. The minimum is six characters. Reenter and confirm the password.

Note The password must include at least three of the following four types of elements: lowercase letters, uppercase letters, numbers, and special characters.

Step 7 In the *Groups Assigned to this User* section, select the **LobbyAmbassador** check box to access the Lobby Ambassador Defaults tab.

Step 8 Follow the steps in the "Setting the Lobby Ambassador Defaults" section on page 6-6.

Managing NCS Guest User Accounts

NCS guest user accounts are managed with the use of templates. This section describes how to manage NCS user accounts. It contains the following topics:

- Printing or E-mailing NCS Guest User Details, page 6-13
- Saving Guest Accounts on a Device, page 6-14

Scheduling NCS Guest User Accounts

A lobby ambassador is able to schedule automatic creation of a guest user account. The validity and recurrence of the account can be defined. The generation of a new password on every schedule is optional and is enabled by selecting a check box. For scheduled users, the password is automatically generated and is automatically sent by e-mail to the host of the guest. The e-mail address for the host is configured on the New User page. After clicking Save, the Guest User Details page displays the password. From this page, you can e-mail or printer the account credentials.

To schedule a recurring guest user account in NCS, follow these steps:

Step 1 Log in to the NCS user interface as lobby ambassador.

Step 2 Choose **Schedule Guest User** from the Guest User page.

Note You can also schedule guest users from the Configure > Controller Template Launch Pad > Security > Guest User option.

Step 3 In the Guest Users > Scheduling page, enter the guest username. The maximum is 24 characters.

Step 4 Select the check box to generate a username and password on every schedule. If this is enabled, a different password is supplied for each day (up to the number of days chosen). If this is disabled (unselected), one password is supplied for a span of days. The generation of a new password on every schedule is optional.

Step 5 Select a Profile ID from the drop-down list. This is the SSID to which this guest user applies and must be a WLAN that has Layer 3 authentication policy configured. Your administrator can advise which Profile ID to use.

Step 6 Enter a description of the guest user account.

Step 7 Choose **limited** or **unlimited**.

- Limited—From the drop-down list, choose days, hours, or minutes for the lifetime of this guest user account. The maximum is 35 weeks.
  - Start time—Date and time when the guest user account begins.
  - End time—Date and time when the guest user account expires.
- Unlimited—This user account never expires.
- Days of the week—Select the check box for the days of the week that apply to this guest user account.

Step 8 Choose **Apply To** to restrict a guest user to a confined area by selecting a campus, building, or floor so that when applied, only those controllers and associated access points are available. You can use AP grouping to enforce access point level restrictions that determine which SSIDs to broadcast. Those access points are then assigned to the respective floors. You can also restrict the guest user to specific listed controllers or a configuration group, which is a group of controllers that has been preconfigured by the administrator.

From the drop-down lists, choose one of the following:

- **Controller List**—Select the check box for the controller(s) to which the guest user account is associated.
- **Indoor Area**—Choose the applicable campus, building, and floor.
- **Outdoor Area**—Choose the applicable campus and outdoor area.
- **Config group**—Choose the configuration group to which the guest user account belongs.

Step 9 Enter the e-mail address to send the guest user account credentials. Each time the scheduled time comes up, the guest user account credentials are e-mailed to the specified e-mail address.

Step 10 Review the disclaimer information. Use the scroll bar to move up and down.

Step 11 Click **Save** to save your changes or **Cancel** to leave the settings unchanged.

Printing or E-mailing NCS Guest User Details

The lobby ambassador can print or e-mail the guest user account details to the host or person who welcomes guests.

The e-mail and print copy shows the following details:

- Username—Guest user account name.
- Password—Password for the guest user account.
- Start time—Data and time when the guest user account begins.
- End time—Date and time when the guest user account expires.
- Profile ID—Profile assigned to the guest user. Your administrator can advise which Profile ID to use.
- Disclaimer—Disclaimer information for the guest user.

When creating the guest user account and applying the account to a list of controllers, area, or configuration group, a link is provided to e-mail or print the guest user account details. You can also print guest user account details from the Guest Users List page.

To print guest user details from the Guest Users List page, follow these steps:

Step 1 Log into the NCS user interface as lobby ambassador.

Step 2 On the Guest User page, select the check box next to User Name, choose **Print/E-mail User Details** from the Select a command drop-down list, and click **Go**.

- If printing, click **Print** and from the print page, select a printer, and click **Print** or **Cancel**.
- If e-mailing, click **E-mail** and from the e-mail page, enter the subject text and the e-mail address of the recipient. Click **Send** or **Cancel**.

Note You can also print or e-mail user details from the Configure > Controller Template Launch Pad > Security > Guest User option.

Saving Guest Accounts on a Device

Select the **Save Guest Accounts on Device** check box to save guest accounts to a WLC flash so that they are maintained across WLC reboots.

Note In the Configure > Controller Template Launch Pad > Security > Guest page, you choose **Save Guest Accounts on device** from the Select a command drop-down list.

Editing the Guest User Credentials

Click the NCS username of the guest user whose credentials you want to edit. The Lobby Ambassador Default tab appears, and you can modify the credentials.

While editing, if the *Profile* selection is removed (changed to *Select a profile*), the defaults are removed for this Lobby Ambassador. The user must reconfigure the defaults to reinforce them.

Adding a New User

The Add User page allows the administrator to set up a new user login including username, password, groups assigned to the user, and virtual domains for the user.

Note You can only assign virtual domains to a newly created user which you own. By assigning virtual domains to a user, the user is restricted to information applicable to those virtual domains.

This section contains the following topics:

Adding User Names, Passwords, and Groups

To add a new user, follow these steps:

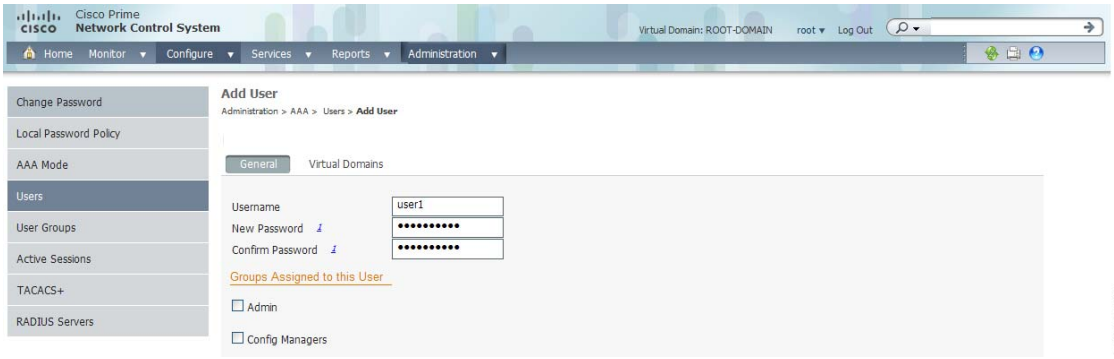
Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 From the Select a command drop-down list, choose **Add User**.

Step 4 Click **Go**. The Users page appears (see Figure 6-5).

Figure 6-5 Users Page



Step 5 Enter a new **Username**.

Step 6 Enter and confirm a password for this account.

Step 7 Select the check box(es) of the groups to which this user is assigned.

Note If the user belongs to Lobby Ambassador, Monitor Lite, Northbound API, or Users Assistant group, the user cannot belong to any other group.

- Admin—Allows users to monitor and configure NCS operations and perform all system administration tasks.
- ConfigManagers—Allows users to monitor and configure NCS operations.
- System Monitoring—Allows users to monitor NCS operations.
- Users Assistant—Allows local net user administration only.
- Lobby Ambassador—Allows guest access for configuration and management only of user accounts. If Lobby Ambassador is selected, a Lobby Ambassador Defaults tab appears.
- Monitor Lite—Allows monitoring of assets location.
- North Bound API User—A user group used by the NCS Web Service consumers. That is, any North Bound APIs.

Note If you are creating a North Bound API user from TACACS or RADIUS, the default user domain should be *root*.

Note North Bound API Users cannot be assigned a Virtual Domain. When a North Bound API group is selected, the Virtual Domains tab is not available.

- SuperUsers—Allows users to monitor and configure NCS operations and perform all system administration tasks including administering NCS user accounts and passwords. Superuser tasks can be changed.
- Root—This group is only assignable to 'root' user and that assignment cannot be changed.

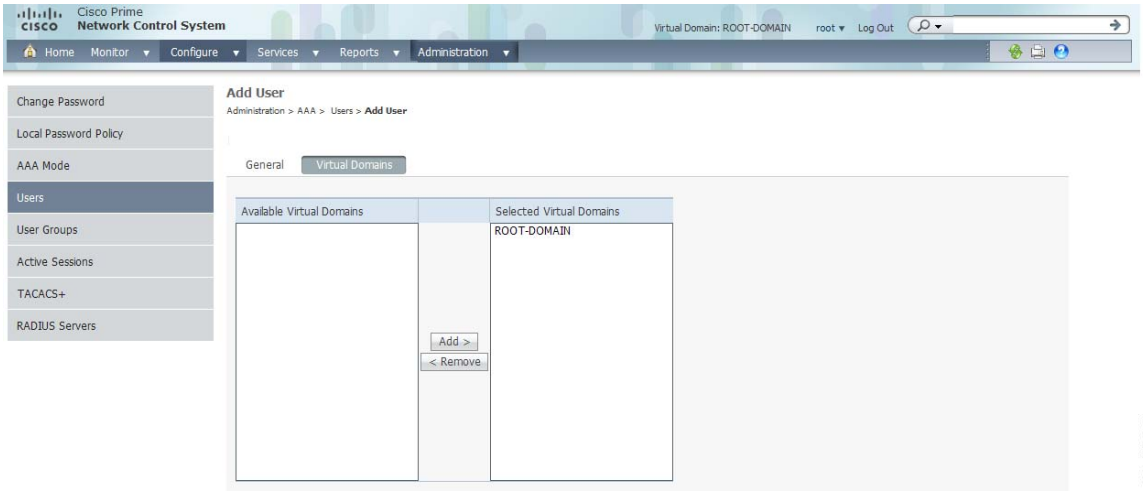
- User Defined.

Assigning a Virtual Domain

To assign a virtual domain to this user, follow these steps:

Step 1 Click the **Virtual Domains** tab. This tab displays all virtual domains available and assigned to this user (see Figure 6-6).

Figure 6-6 Users Virtual Domains Tab



Note The Virtual Domains tab enables the administrator to assign virtual domains for each user. By assigning virtual domains to a user, the user is restricted to information applicable to those virtual domains.

Note North Bound API Users cannot be assigned a Virtual Domain. When a North Bound API group is selected, the Virtual Domains tab is not available.

Step 2 Click to highlight the virtual domain in the Available Virtual Domains list that you want to assign to this user.

Note You can select more than one virtual domain by holding down the Shift or Control key.

Step 3 Click **Add >**. The virtual domain moves from the Available Virtual Domains to the Selected Virtual Domains list.

To remove a virtual domain from the Selected Virtual Domains list, click to highlight the domain in the Selected Virtual Domains list, and click **Remove**. The virtual domain moves from the Selected Virtual Domains to the Available Virtual Domains list.

Step 4 Click **Submit** to save the changes or **Cancel** to close the page without adding or editing the current user.

Managing Lobby Ambassador Accounts

You can use the Cisco Lobby Ambassador to create guest user accounts in NCS. A guest network provided by an enterprise allows access to the Internet for a guest without compromising the host. The web authentication is provided with or without a supplicant or client, so a guest needs to initiate a VPN tunnel to their desired destinations.

Both wired and wireless guest user access is supported. Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

The network administrator must first set up a lobby ambassador account. Guest user accounts are for visitors, temporary workers, and so on. who need network access. A lobby ambassador account has limited configuration privileges and only allows access to the pages used to configure and manage guest user accounts.

The lobby ambassador can create the following types of guest user accounts:

- A guest user account with a limited lifetime. After the specified time period, the guest user account automatically expires.
- A guest user account with an unlimited lifetime. This account never expires.
- A guest user account that is activated at a predefined time in the future. The lobby ambassador defines the beginning and end of the valid time period.

This section contains the following topics:

Creating a Lobby Ambassador Account

Note A group that has the SuperUser/administrator privileges (by default) can create a lobby ambassador account.

To create a lobby ambassador account in NCS, follow these steps:

Step 1 Log into the NCS user interface as an administrator.

Step 2 Choose **Administration > AAA**.

Step 3 From the left sidebar menu, choose **Users**.

Step 4 From the Select a command drop-down list, choose **Add User**.

Step 5 Click **Go**.

Step 6 Enter the username.

Step 7 Enter the password. Reenter to confirm the password. Password requirements include the following:

- The password must have a minimum of eight characters.
- The password must include at least three of the following elements: lowercase letters, uppercase letters, numbers, or special characters.

Step 8 In the Groups Assigned to this User section, select the **LobbyAmbassador** check box to access the Lobby Ambassador Defaults tab.

The Lobby Ambassador Defaults tab has the following parameters:

- Profile—The default profile to which the guest users would connect.
- Lifetime—Limited or Unlimited.

Note By default, the lifetime is limited to eight hours.

- Apply to—From the drop-down list, choose one of the following:
  - **Indoor Area**—Campus, Building, and Floor.
  - **Outdoor Area**—Campus, Outdoor Area.
  - **Controller List**—List of controller(s) on which the selected profile is created.
  - **Config Groups**—Config group names configured on NCS.
- Email ID—The e-mail ID of the host to whom the guest account credentials are sent.
- Description—A brief description of this account.
- Disclaimer—The default disclaimer text.
- Defaults Editable—Select this check box if you want to allow the lobby ambassador to override these configured defaults. This allows the lobby ambassador to modify these Guest User Account default settings while creating Guest Accounts from the Lobby Ambassador portal.

Note If no default profile is selected on this tab, the defaults are not applied to this Lobby Ambassador. However, the Lobby Ambassador account is created and the Lobby Ambassador can create users with credentials as desired.

- Max User Creation Allowed—Select this check box to set limits on the number of guest users that can be created by the Lobby Ambassador in a given time period. The time period is defined in hours, days, or weeks.
- Click **Submit**. The name of the new lobby ambassador account is listed and the account can be used immediately.

Editing a Lobby Ambassador Account

The Lobby Ambassador default credentials can be edited from the username link on the NCS user list page.

To edit the Lobby Ambassador default credentials, follow these steps:

Step 1 Log into the NCS user interface as an administrator.

Step 2 Choose **Administration > AAA**.

Step 3 From the left sidebar menu, choose **Users**.

Step 4 Click the applicable Lobby Ambassador account in the User Name column.

Step 5 From the Lobby Ambassador Defaults page, edit the credentials as necessary.

Note While editing, if the Profile selection is removed (changed to Select a profile), the defaults are removed for this Lobby Ambassador. The user must reconfigure the defaults to reinforce them.

Step 6 Click **Submit**.

Logging in to the NCS User Interface as a Lobby Ambassador

When you log in as a lobby ambassador, you have access to the guest user template page in NCS. You can then configure guest user accounts (through templates).

To log into the NCS user interface through a web browser, follow these steps:

Step 1 Launch Internet Explorer 7.0 or later on your computer.

Note Some NCS features might not function properly if you use a web browser other than Internet Explorer 7.0 or later on a Windows workstation.

Step 2 In the browser address line, enter **https://*NCS-ip-address*** (such as https://1.1.1.1), where *NCS-ip-address* is the IP address of the computer on which NCS is installed. Your administrator can provide this IP address.

Step 3 When the NCS user interface displays the Login window, enter your username and password.

Note All entries are case sensitive.

Note The lobby ambassador can only define guest users templates.

Step 4 Click **Submit** to log into NCS. The NCS user interface is now active and available for use. The Guest Users page is displayed. This page provides a summary of all created Guest Users.

To exit the NCS user interface, close the browser window or click **Logout** in the upper right corner of the page. Exiting a NCS user interface session does not shut down NCS on the server.

Note When a system administrator stops the NCS server during a NCS session, the session ends, and the web browser displays this message: "`The page cannot be displayed`." Your session does not reassociate to NCS when the server restarts. You must restart the NCS session.

Logging the Lobby Ambassador Activities

The following activities are logged for each lobby ambassador account:

- Lobby ambassador login—NCS logs the authentication operation results for all users.
- Guest user creation—When a lobby ambassador creates a guest user account, NCS logs the guest username.
- Guest user deletion—When a lobby ambassador deletes the guest user account, NCS logs the deleted guest username.
- Account updates—NCS logs the details of any updates made to the guest user account. For example, increasing the life time.

To view the lobby ambassador activities, follow these steps:

Note You must have administrative permissions to open this window.

Step 1 Log into the NCS user interface as an administrator.

Step 2 Choose **Administration > AAA > Groups** from the left sidebar menu to display the All Groups page.

Step 3 On the All Groups page, click the **Audit Trail** icon for the lobby ambassador account you want to view. The Audit Trail page for the lobby ambassador appears.

This page enables you to view a list of lobby ambassador activities over time.

- User—User login name
- Operation—Type of operation audited
- Time—Time operation was audited
- Status—Success or failure

Step 4 To clear the audit trail, choose **Clear Audit Trail** from the Select a command drop-down list, and click **Go**.

CHAPTER 7

Configuring Mobility Groups

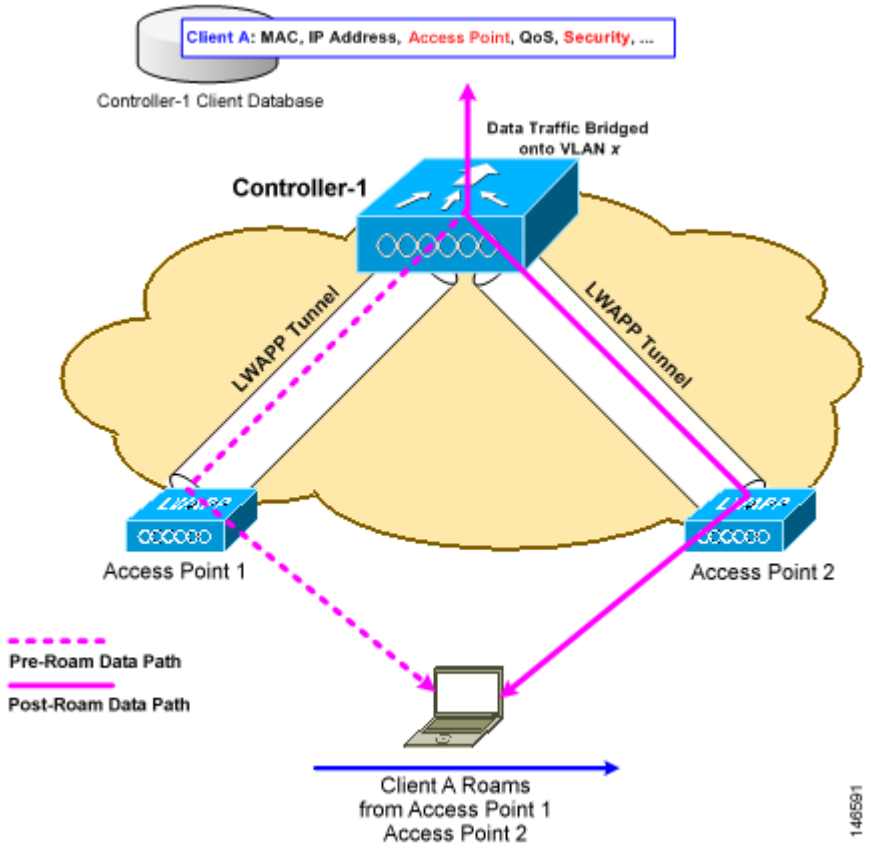
This chapter describes mobility groups and explains how to configure them on Cisco NCS. It contains the following sections:

Information About Mobility

Mobility, or roaming, is an ability of a wireless client to maintain its association seamlessly from one access point to another securely and with as little latency as possible. This section explains how mobility works when controllers are included in a wireless network.

When a wireless client associates and authenticates to an access point, the controller places an entry for that client in its client database. This entry includes the MAC and IP addresses of the client, security context and associations, quality of service (QoS) contexts, the WLANs, and the associated access point. The controller uses this information to forward frames and manage traffic to and from the wireless client. Figure 7-1 illustrates a wireless client roaming from one access point to another when both access points are joined to the same controller.

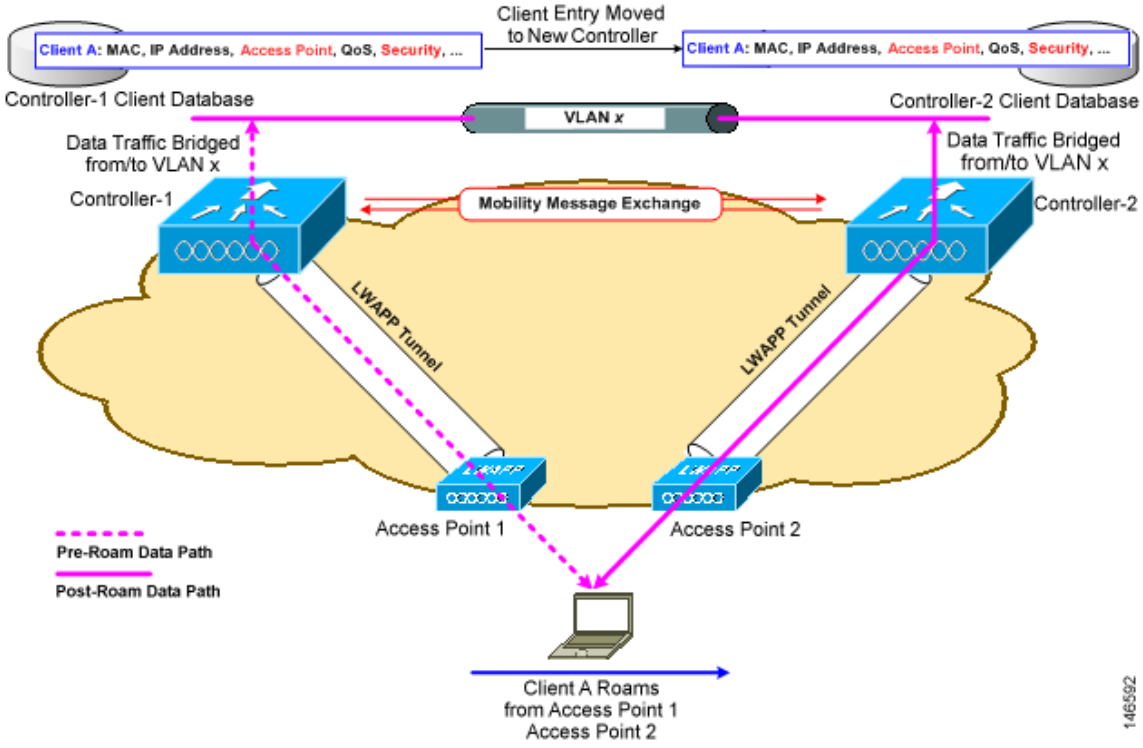
Figure 7-1 Intra-Controller Roaming



When the wireless client moves its association from one access point to another, the controller simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well.

The process becomes more complicated, however, when a client roams from an access point joined to one controller to an access point joined to a different controller. The process also varies based on whether the controllers are operating on the same subnet. Figure 7-2 illustrates *inter-controller roaming*, which occurs when the wireless LAN interfaces of a controller are on the same IP subnet.

Figure 7-2 Inter-Controller Roaming

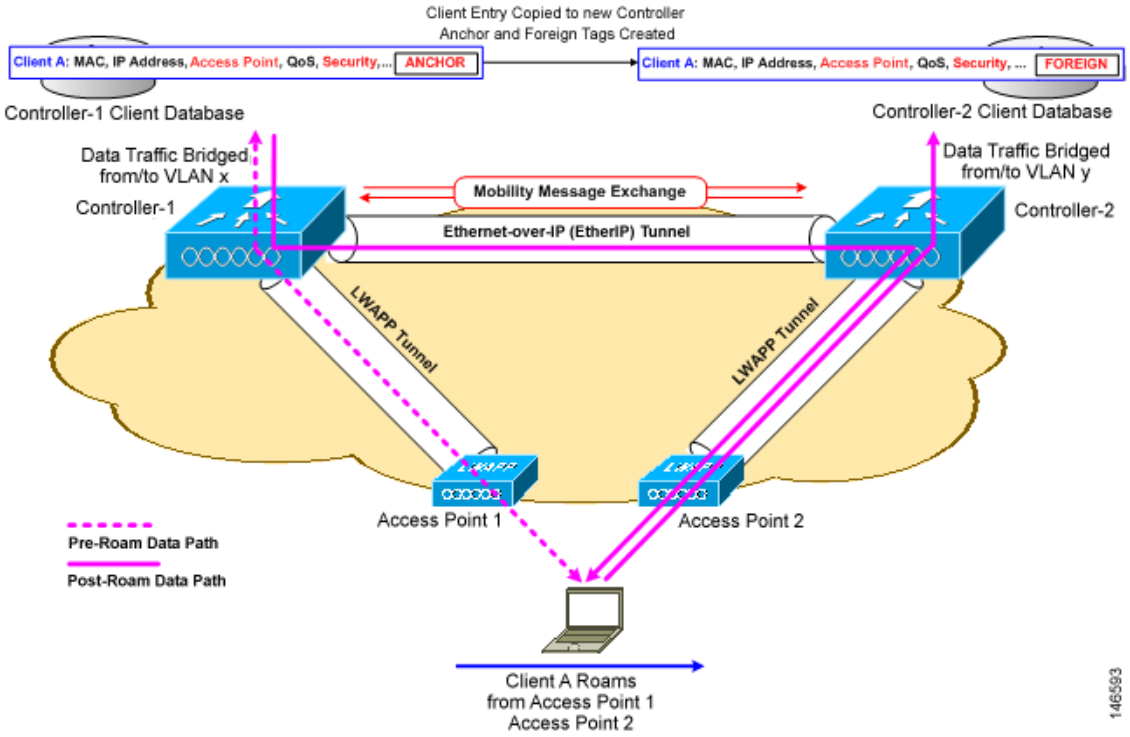


When the client associates to an access point joined to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains invisible to the user.

Note All clients configured with 802.1X/Wi-Fi Protected Access (WPA) security complete a full authentication to comply with the IEEE standard.

Figure 7-3 illustrates *inter-subnet roaming*, which occurs when the wireless LAN interfaces of a controller are on different IP subnets.

Figure 7-3 Inter-Subnet Roaming



Inter-subnet roaming is similar to inter-controller roaming in that the controllers exchange mobility messages on how the client roams. However, instead of moving the client database entry to the new controller, the original controller marks the client with an "Anchor" entry in its own client database. The database entry is copied to the new controller client database and marked with a "Foreign" entry in the new controller. The roam remains invisible to the wireless client, and the client maintains its original IP address.

After an inter-subnet roam, data flows in an asymmetric traffic path to and from the wireless client. Traffic from the client to the network is forwarded directly into the network by the foreign controller. Traffic to the client arrives at the anchor controller, which forwards the traffic to the foreign controller in an EtherIP tunnel. The foreign controller then forwards the data to the client. If a wireless client roams to a new foreign controller, the client database entry is moved from the original foreign controller to the new foreign controller, but the original anchor controller is always maintained. If the client moves back to the original controller, it becomes local again.

In inter-subnet roaming, WLANs on both anchor and foreign controllers need to have the same network access privileges and no source-based routing or source-based firewalls in place. Otherwise, the clients might have network connectivity problems after the handoff.

Note Currently, multicast traffic cannot be passed during inter-subnet roaming. In other words, avoid designing an inter-subnet network for Spectralink phones that need to send multicast traffic while using push to talk.

Note Both inter-controller roaming and inter-subnet roaming require the controllers to be in the same mobility group. See the next two sections for a description of mobility groups and instructions for configuring them.

Symmetric Tunneling

With symmetric mobility tunneling, the controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. The client traffic on the wired network is directly routed by the foreign controller. If a router has Reverse Path Filtering (RPF) enabled (which provides additional checks on incoming packets), the communication is blocked. Symmetric mobility tunneling allows the client traffic to reach the controller designated as the anchor, even with RPF enabled. You enable or disable symmetric tunneling by choosing Configure > Controller and then System > General from the left sidebar menu.

Note All controllers in a mobility group should have the same symmetric tunneling mode.

Note For symmetric tunneling to take effect, a reboot is required.

With this guest tunneling N+1 redundancy feature, the time it takes for a client to join another access point following a controller failure is decreased because a failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

See the "Configuring Controller Templates" section on page 10-4 for instructions on configuring this feature within a template.

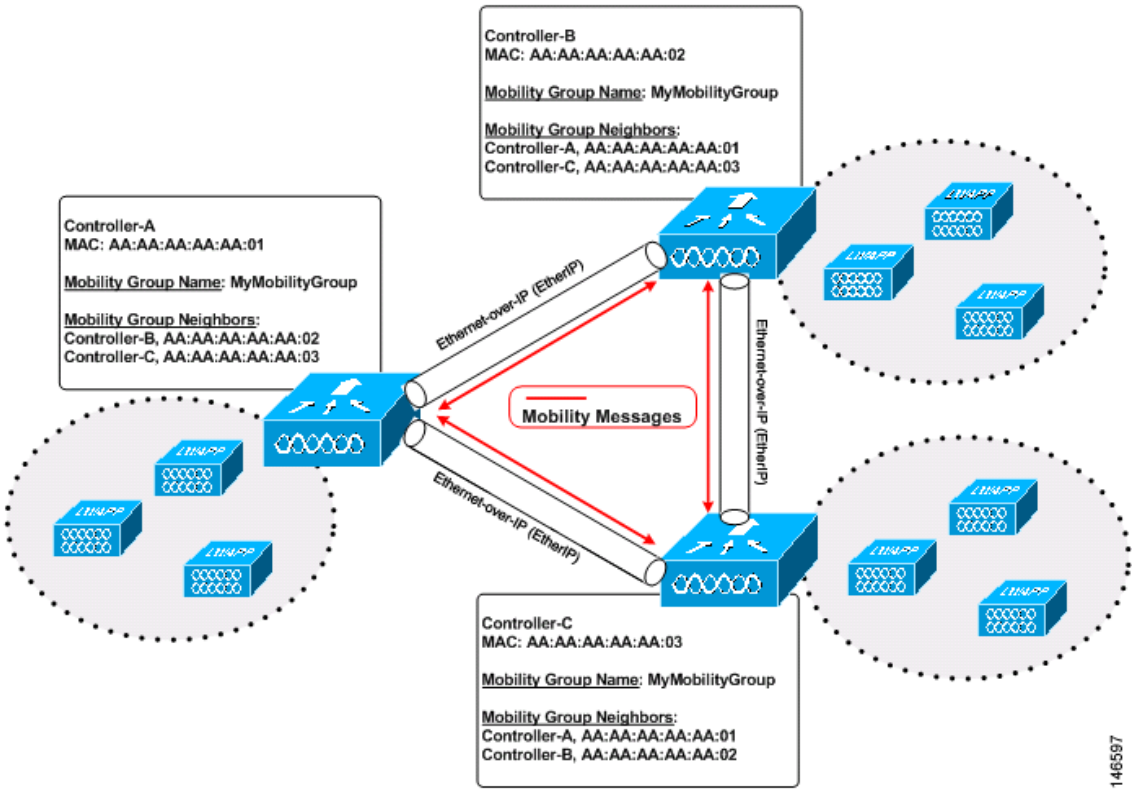
Overview of Mobility Groups

A set of controllers can be configured as a *mobility group* to allow seamless client roaming within a group of controllers. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers can share the context and state of client devices and controller loading information. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.

Note Clients do not roam across mobility groups.

Figure 7-4 shows an example of a mobility group.

Figure 7-4 A Single Mobility Group



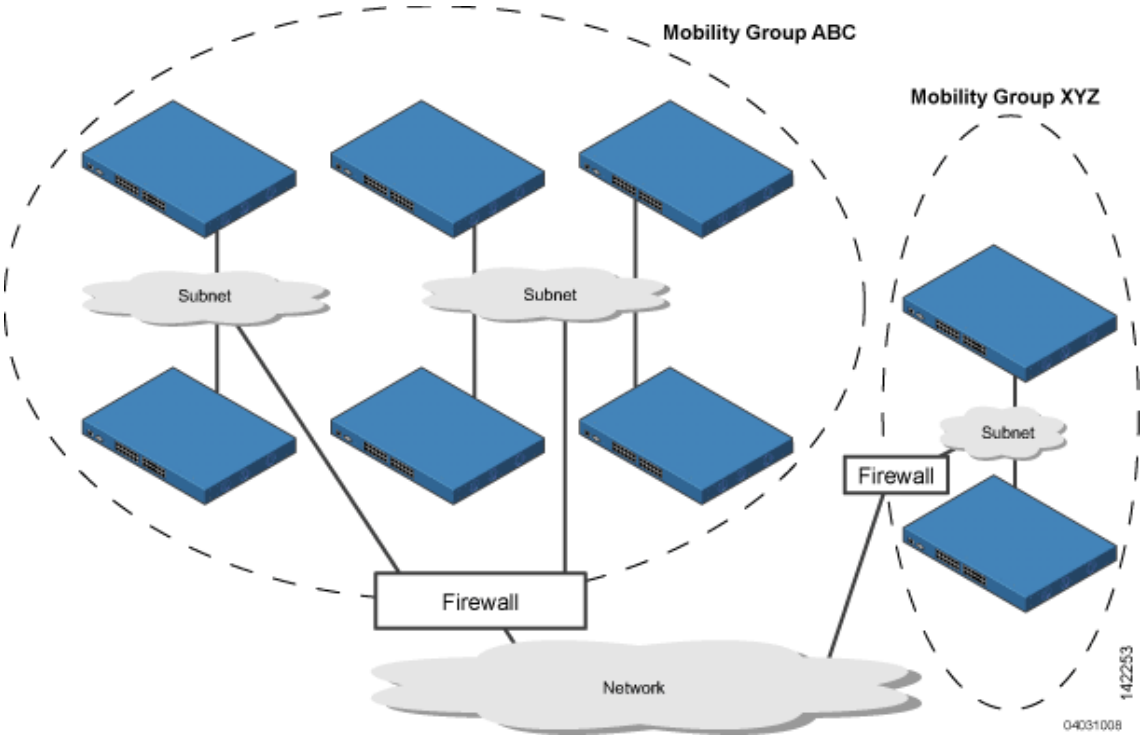
As shown in Figure 7-4, each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client. All mobility exchange traffic between controllers is carried over a CAPWAP tunnel.

Examples:

1. A 4404-100 controller supports up to 100 access points. Therefore, a mobility group consisting of 24 4404-100 controllers supports up to 2400 access points (24 * 100 = 2400 access points).
2. A 4402-25 controller supports up to 25 access points, and a 4402-50 controller supports up to 50 access points. Therefore, a mobility group consisting of 12 4402-25 controllers and 12 4402-50 controllers supports up to 900 access points (12 * 25 + 12 * 50 = 300 + 600 = 900 access points).

Mobility groups enable you to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different mobility group names to different controllers within the same wireless network. Figure 7-5 shows the results of creating distinct mobility group names for two groups of controllers.

Figure 7-5 Two Mobility Groups



The controllers in the ABC mobility group recognize and communicate with each other through their access points and through their shared subnets. The controllers in the ABC mobility group do not recognize or communicate with the XYZ controllers, which are in a different mobility group. Likewise, the controllers in the XYZ mobility group do not recognize or communicate with the controllers in the ABC mobility group. This feature ensures mobility group isolation across the network.

Note Clients might roam between access points in different mobility groups, provided they can detect them. However, their session information is not carried between controllers in different mobility groups.

When to Include Controllers in a Mobility Group

If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be in the same mobility group.

Messaging among Mobility Groups

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers. There can be up to 72 members in the list with up to 24 in the same mobility group. In NCS and controller software releases 5.0, two improvements have been made to mobility messaging, each of which is especially useful when sending messages to the full list of mobility members:

- Sending Mobile Announce messages within the same group first and then to other groups in the list

  The controller sends a Mobile Announce message to members in the mobility list each time a new client associates to it. In NCS and controller software releases prior to 5.0, the controller sends this message to all members in the list irrespective of the group to which they belong. However, in controller software release 5.0, the controller sends the message only to those members that are in the same group as the controller and then includes all of the other members while sending retries.

- Sending Mobile Announce messages using multicast instead of unicast

  In NCS and controller software releases prior to 5.0, the controller might be configured to use multicast to send the mobile announce messages, which requires sending a copy of the messages to every mobility member. This behavior is not efficient because many messages (such as Mobile Announce, PMK Update, AP List Update, and IDS Shun) are meant for all members in the group. In NCS and controller software releases 5.0, the controller uses multicast mode to send the Mobile Announce messages. This behavior allows the controller to send only one copy of the message to the network, which destines it to the multicast group containing all the mobility members. To derive the maximum benefit from multicast messaging, We recommend that it be enabled or disabled on all group members.

Configuring Mobility Groups

This section provides instructions for configuring mobility groups.

Note You can also configure mobility groups using the controller. See the *Cisco Wireless LAN Controller Configuration Guide* for instructions.

Prerequisites

Before you add controllers to a mobility group, you must verify that the following requirements have been met for all controllers that are to be included in the group:

- All controllers must be configured for the same LWAPP transport mode (Layer 2 or Layer 3).

  Note You can verify and, if necessary, change the LWAPP transport mode in the System > General page.

- IP connectivity must exist between the management interfaces of all devices.

  Note You can verify IP connectivity by pinging the controllers.

- All controllers must be configured with the same mobility group name.

  Note For the Cisco WiSM, both controllers should be configured with the same mobility group name for seamless routing among 300 access points.

- All devices must be configured with the same virtual interface IP address.

Note If all the controllers within a mobility group are not using the same virtual interface, inter-controller roaming might appear to work, but the hand-off does not complete, and the client loses connectivity for a period of time.

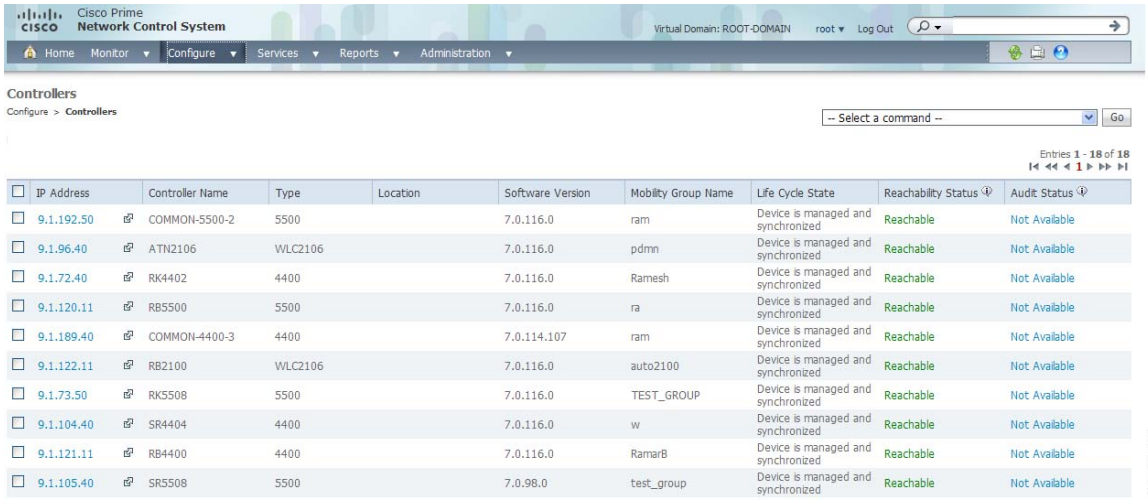
- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you configure all controllers with the MAC address and IP address of all the other mobility group members.

Note You can find the MAC and IP addresses of the other controllers to be included in the mobility group in the Configure > Controllers page.

To add each WLC controller into mobility groups and configure them, follow these steps:

Step 1 Choose **Configure > Controllers** (see Figure 7-6).

Figure 7-6 Configure > Controllers

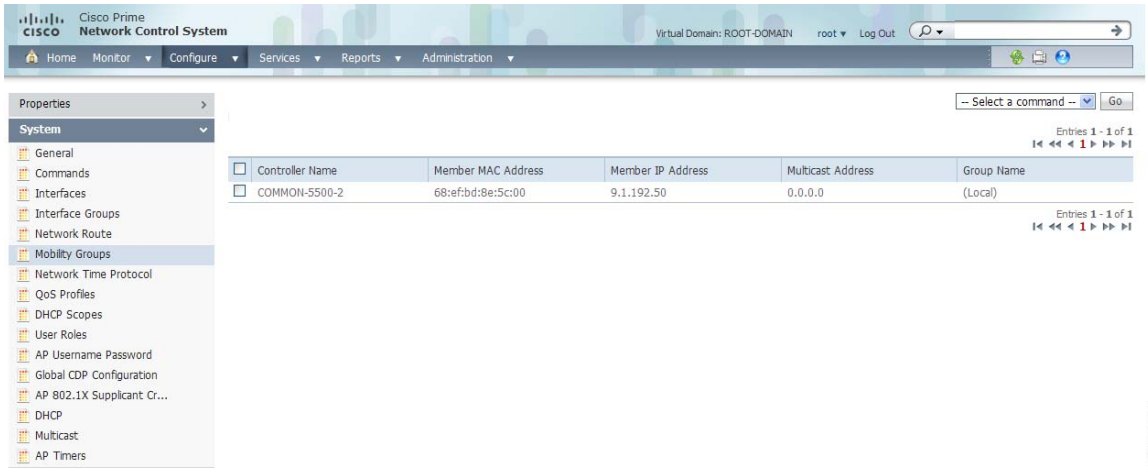


This page shows the list of all the controllers you added in Step 1. The mobility group names and the IP address of each controller that is currently a member of the mobility group is listed.

Step 2 Choose the first controller by clicking the WLC IP address. You then access the controller templates interface for the controller you are managing.

Step 3 Choose **System > Mobility Groups** from the left sidebar menu. The existing Mobility Group members are listed in the page (see Figure 7-7).

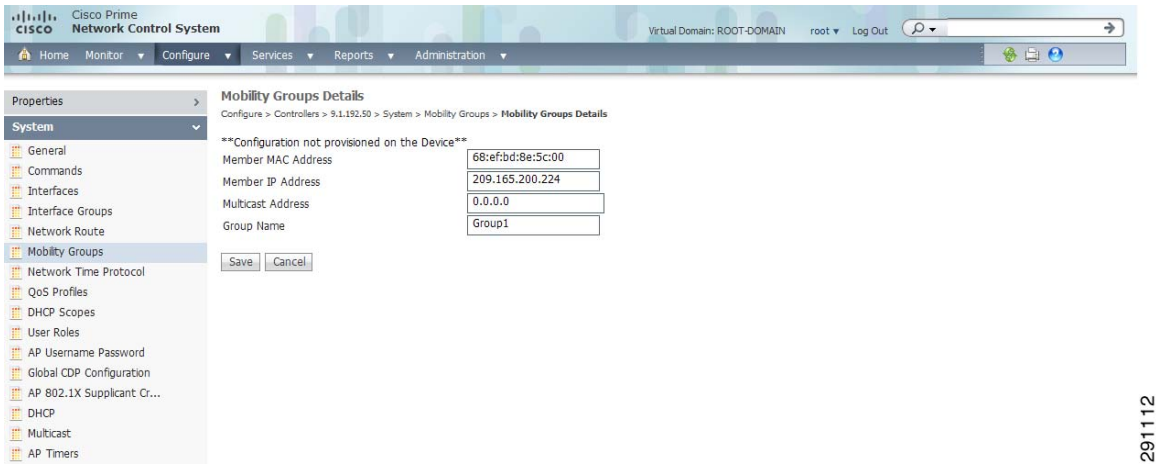
Figure 7-7 Existing Mobility Groups



Step 4 You see a list of available controllers. From the Select a command drop-down list in the upper right-hand corner, choose **Add Group Members** and then click **Go**.

Step 5 If no controllers were found to add to the mobility group, you can add the members manually by clicking the "To add members manually to the Mobility Group click here" link. The Mobility Group Member page appears (see Figure 7-8).

Figure 7-8 Mobility Group Member Page



Step 6 In the Member MAC Address text box, enter the MAC address of the controller to be added.

Step 7 In the Member IP Address text box, enter the management interface IP address of the controller to be added.

Note If you are configuring the mobility group in a network where Network Address Translation (NAT) is enabled, enter the IP address sent to the controller from the NAT device rather than the management interface IP address of the controller. Otherwise, mobility fails among controllers in the mobility group.

Step 8 Enter the multicast group IP address to be used for multicast mobility messages in the Multicast Address text box. The group address of the local mobility member must be the same as the group address of the local controller.

Step 9 In the Group Name text box, enter the name of the mobility group.

Step 10 Click **Save**.

Step 11 Repeat the Steps 1 through 9 for the remaining WLC devices.

Setting the Mobility Scalability Parameters

To set the mobility message parameters, follow these steps:

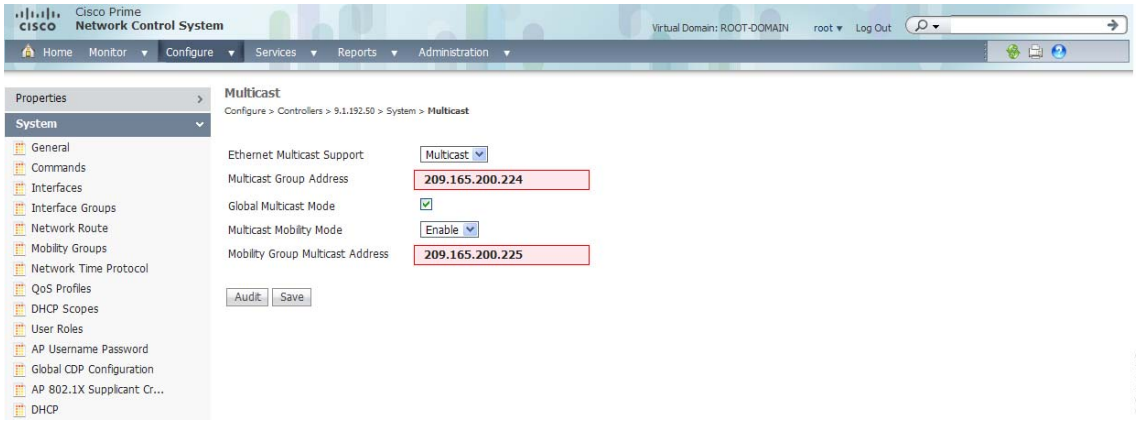
Note You must complete the steps in the "Configuring Mobility Groups" section on page 7-8 prior to setting the mobility scalability parameters.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose an IP address of a controller whose software version is 5.0 or later.

Step 3 Choose **System > Multicast** from the left sidebar menu. The Multicast page appears (see Figure 7-9).

Figure 7-9 Multicast Page



Step 4 From the Ethernet Multicast Support drop-down list, specify if you want to disable the ability for the controller to use multicast mode to send Mobile Announce messages to mobility members. Otherwise, you can choose **Multicast** or **Unicast** from the drop-down list.

Step 5 If you chose multicast in Step 4, you must enter the group IP address at the Multicast Group Address field to begin multicast mobility messaging. You must configure this IP address for the local mobility group, but it is optional for other groups within the mobility list. If you do not configure the IP address for other (non-local) groups, the controllers use unicast mode to send mobility messages to those members.

Step 6 Select the **Global Multicast Mode** check box to make the multicast mode available globally.

Step 7 Select the **Enable IGMP Snooping** check box to enable IGMP snooping.

Step 8 Choose **Enable** from the Multicast Mobility Mode drop-down list to change the IGMP snooping status or to set the IGMP timeout. When IGMP snooping is enabled, the controller gathers IGMP reports from the clients and then sends each access point a list of the clients listening to any multicast group. The access point then forwards the multicast packets only to those clients.

The timeout interval has a range of 3 to 300 and a default value of 60. When the timeout expires, the controller sends a query to all WLANs. Those clients which are listening in the multicast group then send a packet back to the controller.

Step 9 If you enabled the Multicast Mobility Mode, enter the mobility group multicast address.

Step 10 Select the **Multicast Direct** check box to enable videos to be streamed over a wireless network.

Step 11 Specify the Session Banner information, which is the error information sent to the client if the client is denied or dropped from a Media Stream.

a. State—Select the check box to activate the Session Banner. If not activated, the Session Banner is not sent to the client

b. URL—A web address reported to the client

c. Email—An e-mail address reported to the client

d. Phone—A telephone number reported to the client

e. Note—A note reported to the client

Note All media streams on a controller share this configuration.

Step 12 Click **Save**.

Mobility Anchors

Mobility anchors are a subset of a mobility group specified as the anchor controllers for a WLAN. This feature can be used to restrict a WLAN to a single subnet, regardless of the entry point of a client into the network. In this way, users can access a public or guest WLAN throughout an enterprise but still be restricted to a specific subnet. Guest WLAN can also be used to provide geographic load balancing because WLANs can represent a particular section of a building (such as a lobby, a restaurant, and so on).

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the controller is announced to the other controllers in the same mobility group. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated through a mobility tunnel using EtherIP and sent to the anchor controller, where they are decapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EtherIP. The foreign controller decapsulates the packets and forwards them to the client.

Note A 2000 series controller cannot be designated as an anchor for a WLAN. However, a WLAN created on a 2000 series controller can have a 4100 series controller or a 4400 series controller as its anchor.

Note The L2TP Layer 3 security policies are unavailable for WLANs configured with a mobility anchor.

Configuring Mobility Anchors

To create a new mobility anchor for a WLAN, follow these steps:

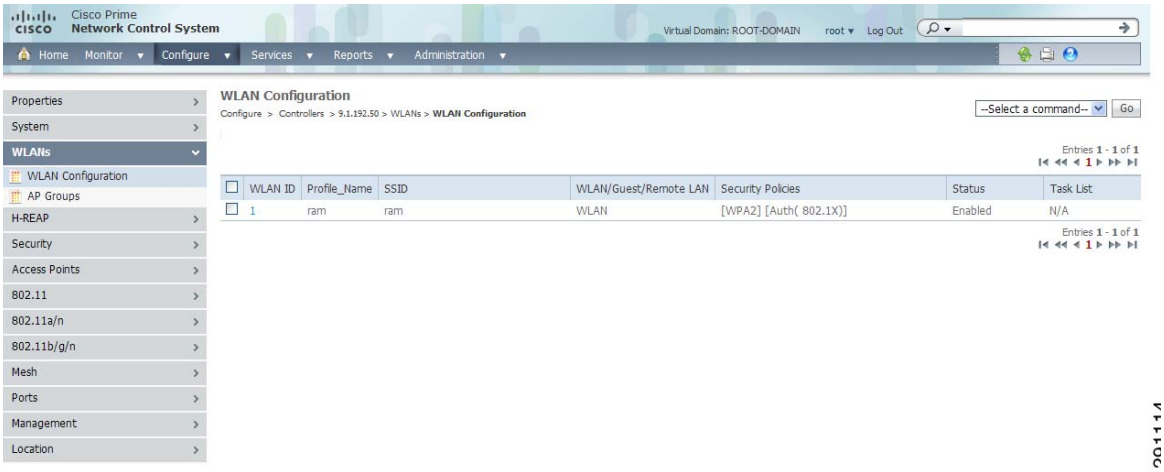
Step 1 Choose **Configure > Controllers**.

Step 2 Choose a controller by clicking an IP address.

Step 3 Choose **WLANs > WLAN Configuration** from the left sidebar menu.

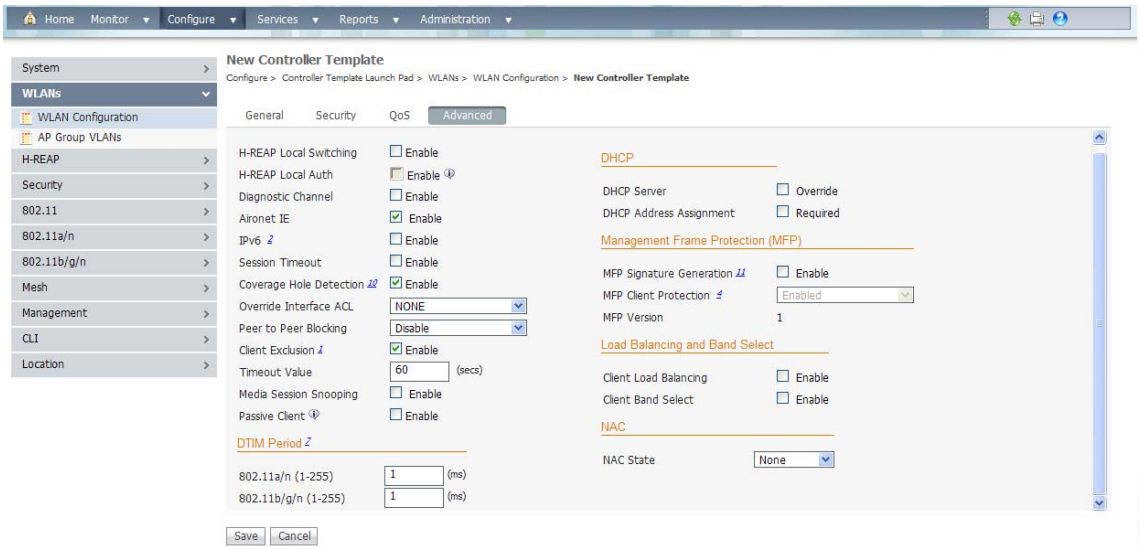
Step 4 Select the check box of the desired WLAN ID URL (see Figure 7-10).

Figure 7-10 WLAN Page



Step 5 After choosing a WLAN ID, a tabbed page appears (see Figure 7-11). Click the **Advanced** tab.

Figure 7-11 Advanced Page



Step 6 Click the **Mobility Anchors** link at the bottom of the page. The Mobility Anchors page appears.

Step 7 Select the **IP address** check box of the controller to be designated a mobility anchor, and click **Save**.

Step 8 Repeat Step 6 and Step 7 to set any other controllers as anchors for this WLAN.

Step 9 Configure the same set of anchor controllers on every controller in the mobility group.

Configuring Multiple Country Codes

You can configure one or more countries on a controller. After countries are configured on a controller, the corresponding 802.11a/n DCA channels are available for selection. At least one DCA channel must be selected for the 802.11a/n network. When the country codes are changed, the DCA channels are automatically changed in coordination.

Note 802.11a/n and 802.11b/n networks for controllers and access points must be disabled before configuring a country on a controller. To disable 802.11a/n or 802.11b/n networks, choose **Configure > Controllers**, select the desired controller you want to disable, choose **802.11a/n** or **802.11b/g/n** from the left sidebar menu, and then choose **Parameters**. The Network Status is the first check box.

Note To configure multiple country codes outside of a mobility group, see the "Configuring Security Parameters" section on page 8-85.

To add multiple controllers that are defined in a configuration group and then set the DCA channels, follow these steps:

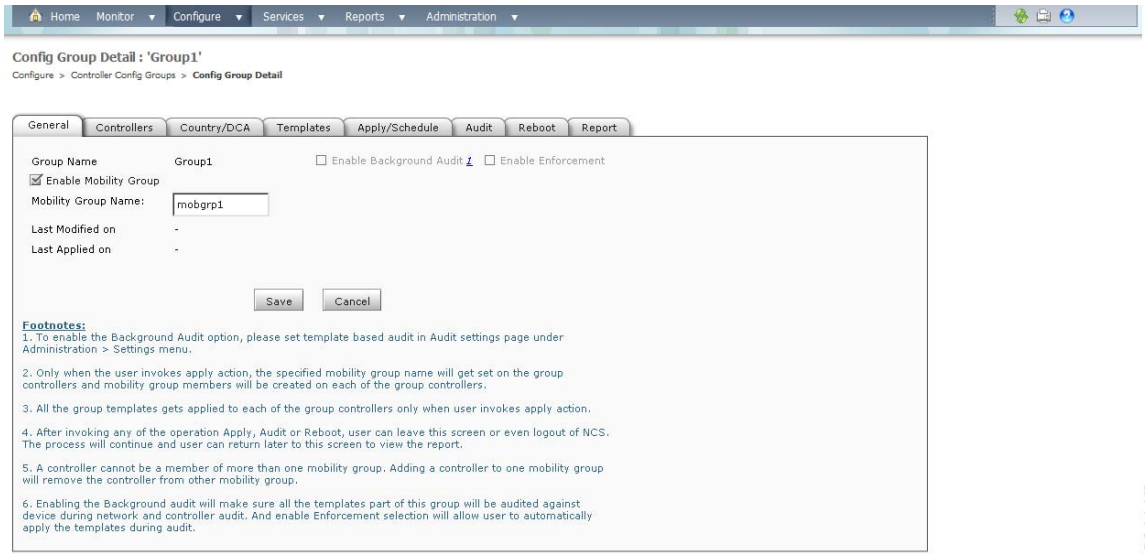
Step 1 Choose **Configure > Controller Config Groups**.

Step 2 Choose **Add Config Groups** from the Select a command drop-down list, and click **Go**.

Step 3 Create a config group by entering the group name and mobility group name.

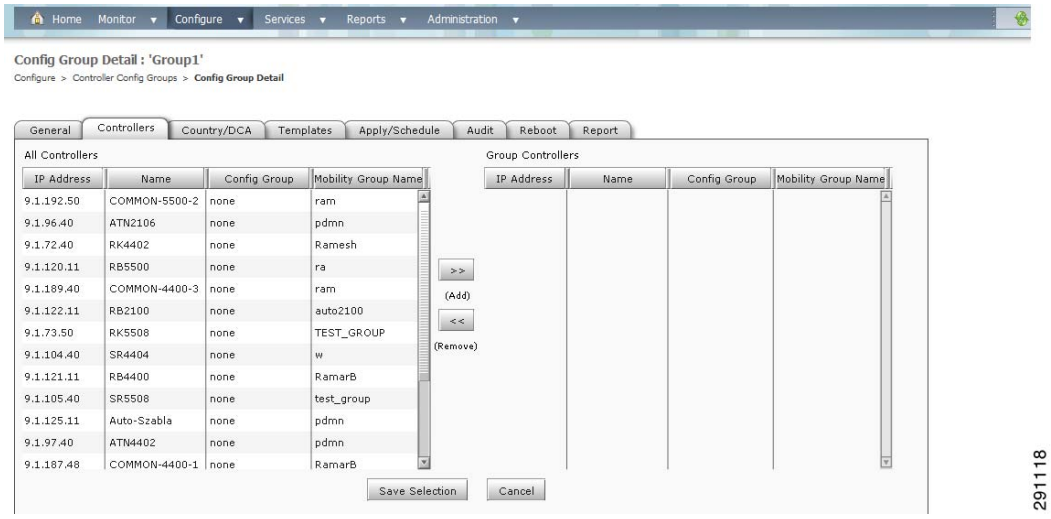
Step 4 Click **Save**. The Config Groups page appears (see Figure 7-12).

Figure 7-12 Config Groups Page



Step 5 Click the **Controllers** tab. The Controllers page appears (see Figure 7-13).

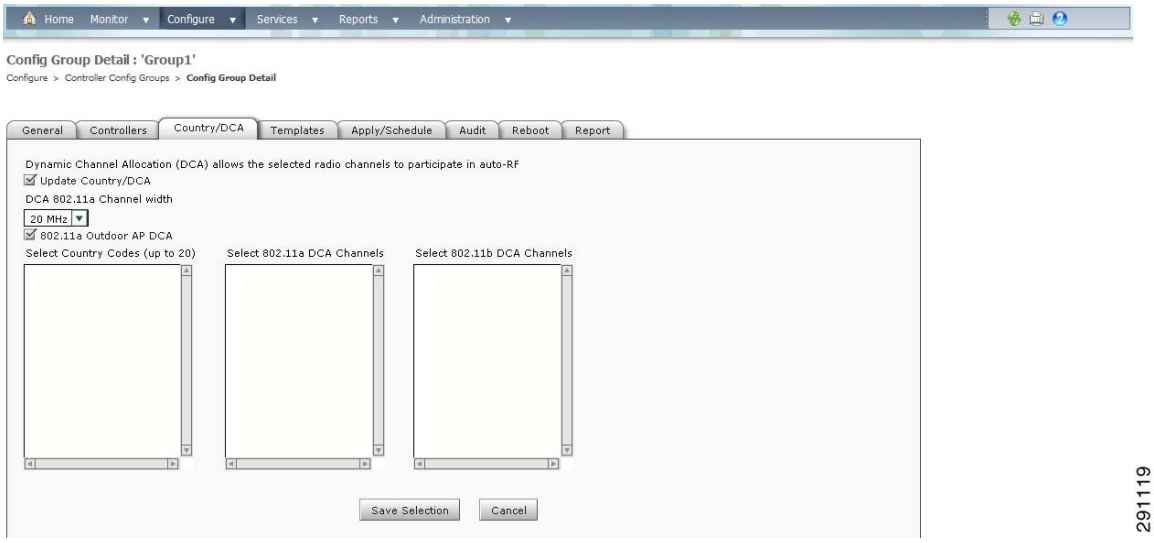
Figure 7-13 Controllers Tab



Step 6 Highlight the controllers you want to add, and click **Add**. The controller is added to the Group Controllers page.

Step 7 Click the **Country/DCA** tab. The Country/DCA page appears (see Figure 7-14). Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

Figure 7-14 Country/DCA Tab



Step 8 Select the **Update Country/DCA** check box to display a list of countries from which to choose.

Step 9 Those DCA channels that are currently configured on the controller for the same mobility group are displayed in the Select Country Codes page. The corresponding 802.11a/n and 802.11b/n allowable channels for the chosen country is displayed as well. You can add or delete any channels in the list by selecting or deselecting the channel and clicking **Save Selection**.

Note A minimum of 1 and a maximum of 20 countries can be configured for a controller.

Configuring Controller Config Groups

By creating a config group, you can group controllers that should have the same mobility group name and similar configuration. You can assign templates to the group and push templates to all the controllers in a group. You can add, delete, or remove config groups, and download software, IDS signatures, or a customized web authentication page to controllers in the selected config groups. You can also save the current configuration to nonvolatile (flash) memory to controllers in selected config groups.

Note A controller cannot be a member of more than one mobility group. Adding a controller to one mobility group removes that controller from any other mobility group to which it is already a member.

For information about applying templates to either individual controllers or controllers in selected Config Groups, see the "Using Templates" section on page 10-1.

By choosing Configure > Controller Config Groups, you can view a summary of all config groups in the NCS database. When you choose Add Config Groups from the Select a command drop-down list, the page displays a table with the following columns:

- Group Name: Name of the config group.

- Templates: Number of templates applied to config group.

Adding New Group

To add a config group, follow these steps:

Step 1 Choose **Configure > Controller Config Groups**.

Step 2 From the Select a command drop-down list, choose **Add Config Group**, and click **Go**. The Add New Group page appears.

Step 3 Enter the new config group name. It must be unique across all groups. If Enable Background Audit is selected, the network and controller audits occur for this config group. If Enable Enforcement is selected, the templates are automatically applied during the audit if any discrepancies are found.

Note If the Enable Background Audit option is chosen, the network and controller audit is performed on this config group.

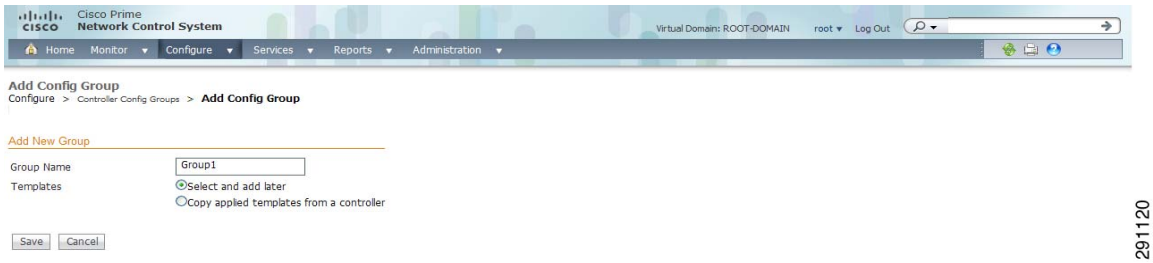
Step 4 Other templates created in NCS can be assigned to a config group. The same WLAN template can be assigned to more than one config group. Choose from the following:

- Select and add later: Click to add a template at a later time.
- Copy templates from a controller: Click to copy templates from another controller. Choose a controller from a list of current controllers to copy its applied template to the new config group. Only the templates are copied.

Note The order of the templates is important when dealing with radio templates. For example, if the template list includes radio templates that require the radio network to be disabled prior to applying the radio parameters, the template to disable the radio network must be added to the template first.

Step 5 Click **Save**. The Config Groups page appears (see Figure 7-15).

Figure 7-15 Config Groups Page



Configuring Config Groups

To configure a config group, follow these steps:

Step 1 Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column. The Config Group page shown in Figure 7-15 appears.

Step 2 Click the **General** tab. The following options for the config group appear:

- Group Name: Name of the config group
  - Enable Background Audit—If selected, all the templates that are part of this group are audited against the controller during network and controller audits.
  - Enable Enforcement—If selected, the templates are automatically applied during the audit if any discrepancies are found.

    Note The audit and enforcement of the config group template happens when the selected audit mode is *Template based audit*.

  - Enable Mobility Group—If selected, the mobility group name is pushed to all controllers in the group.
- Mobility Group Name: Mobility Group Name that is pushed to all controllers in the group. The Mobility Group Name can also be modified here.

  Note A controller can be part of multiple config groups.

- Last Modified On: Date and time config group was last modified.
- Last Applied On: Date and time last changes were applied.

Step 3 You must click the **Apply/Schedule** tab to distribute the specified mobility group name to the group controllers and to create mobility group members on each of the group controllers.

Step 4 Click **Save**.

Adding or Removing Controllers from a Config Group

To add or remove controllers from a config group, follow these steps:

Step 1 Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.

Step 2 Click the **Controllers** tab. The columns in the table display the IP address of the controller, the config group name the controller belongs to, and the mobility group name of the controller.

Step 3 Click to highlight the row of the controller you want to add to the group.

Step 4 Click **Add**.

Note If you want to remove a controller from the group, highlight the controller in the Group Controllers box and click **Remove**.

Step 5 You must click the **Apply/Schedule** tab, and click **Apply** to add or remove the controllers to the config groups.

Step 6 Click **Save Selection**.

Adding or Removing Templates from the Config Group

To add or remove templates from the config group, follow these steps:

Step 1 Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.

Step 2 Click the **Templates** tab. The Remaining Templates table displays the item number of all available templates, the template name, and the type and use of the template.

Step 3 Click to highlight the row of the template you want to add to the group.

Step 4 Click **Add** to move the highlighted template to the Group Templates column.

Note If you want to remove a template from the group, highlight the template in the Remaining Templates box, and click **Remove**.

Step 5 You must click the **Apply/Schedule** tab, and click **Apply** to add or remove the templates to the config groups.

Step 6 Click **Save Selection**.

Applying or Scheduling Config Groups

Note The scheduling function allows you to schedule a start day and time for provisioning.

To apply the mobility groups, mobility members, and templates to all the controllers in a config group, follow these steps:

Step 1 Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.

Step 2 Click the **Apply/Schedule** tab to access this page.

Step 3 Click **Apply** to start the provisioning of mobility groups, mobility members, and templates to all the controllers in the config group. After you apply, you can leave this page or log out of NCS. The process continues, and you can return later to this page to view a report.

Note Do not perform any other config group functions during the apply provisioning.

A report is generated and appears in the Recent Apply Report page. It shows which mobility group, mobility member, or template were successfully applied to each of the controllers.

Note If you want to print the report as shown on the page, you must choose landscape page orientation.

Step 4 Enter a starting date in the text box or use the calendar icon to choose a start date.

Step 5 Choose the starting time using the hours and minutes drop-down lists.

Step 6 Click **Schedule** to start the provisioning at the scheduled time.

Auditing Config Groups

The Config Groups Audit page allows you to verify if the configuration complies of the controller with the group templates and mobility group. During the audit, you can leave this screen or log out of NCS. The process continues, and you can return to this page later to view a report.

Note Do not perform any other config group functions during the audit verification.

To perform a config group audit, follow these steps:

Step 1 Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.

Step 2 Click the **Audit** tab to access this page.

Step 3 Click to highlight a controller from the Controllers tab, choose **>> (Add)**, and **Save Selection**.

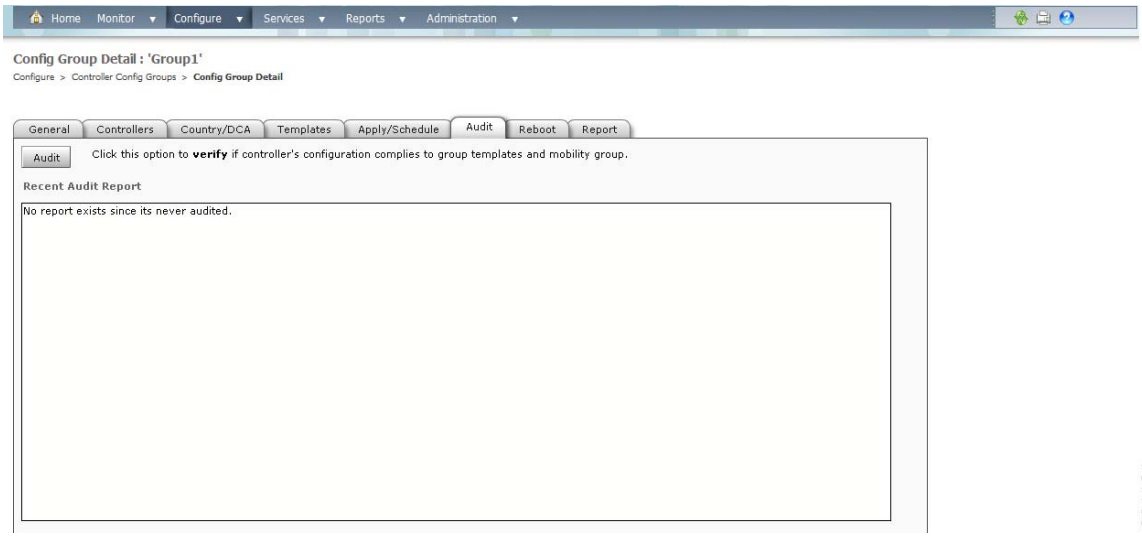
Step 4 Click to highlight a template from the Templates tab, choose **>> (Add)**, and **Save Selection**.

Step 5 Click **Audit** to begin the auditing process (see Figure 7-16).

A report is generated and the current configuration on each controller is compared with that in the config group templates. The report displays the audit status, the number of templates in sync, and the number of templates out of sync.

Note This audit does not enforce the NCS configuration to the device. It only identifies the discrepancies.

Figure 7-16 Config Groups Audit Tab



Step 6 Click **Details** to view the Controller Audit Report details.

Step 7 Double-click a line item to open the Attribute Differences page. This page displays the attribute, its value in NCS, and its value in the controller.

Note Click **Retain NCS Value** to push all attributes in the Attribute Differences page to the device.

Step 8 Click **Close** to return to the Controller Audit Report page.

Rebooting Config Groups

To reboot a config group, follow these steps:

Step 1 Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.

Step 2 Click the **Reboot** tab.

Step 3 Select the **Cascade Reboot** check box if you want to reboot one controller at a time, waiting for that controller to come up before rebooting the next controller.

Step 4 Click **Reboot** to reboot all controllers in the config group at the same time. During the reboot, you can leave this page or logout of NCS. The process continues, and you can return later to this page and view a report.

The Recent Reboot Report page shows when each controller was rebooted and what the controller status is after the reboot. If NCS is unable to reboot the controller, a failure is shown.

Note If you want to print the report as shown on the page, you must choose landscape page orientation.

Reporting Config Groups

To display all recently applied reports under a specified group name, follow these steps:

Step 1 Choose **Configure > Controller Config Groups**, and click a group name in the Group Name column.

Step 2 Click the **Report** tab. The Recent Apply Report page displays all recently applied reports including the apply status, the date and time the apply was initiated, and the number of templates. The following information is provided for each individual IP address:

- Apply Status—Indicates success, partial success, failure, or not initiated.
- Successful Templates—Indicates the number of successful templates associated with the applicable IP address.
- Failures—Indicates the number of failures with the provisioning of mobility group, mobility members, and templates to the applicable controller.
- Details—Click **Details** to view the individual failures and associated error messages.

Step 3 If you want to view the scheduled task reports, click the **click here** link at the bottom of the page. You are then redirected to the Configure > Scheduled Configuration Tasks > Config Group menu where you can view reports of the scheduled config groups.

Downloading Software

To download software to all controllers in the selected groups after you have a config group established, follow these steps:

Step 1 Choose **Configure > Controller Config Groups**.

Step 2 Select the check box to choose one or more config groups names on the Config Groups page.

Step 3 Choose **Download Software** from the Select a command drop-down list, and click **Go**.

Step 4 The Download Software to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed. Choose **local machine** from the File is Located On field.

Step 5 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries field.

Step 6 Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout field.

Step 7 The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** to navigate to it. The controller uses this local filename as a base name and then adds _custom.sgi as a suffix.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried.

Step 8 Click **OK**.

Downloading IDS Signatures

To download Intrusion Detection System (IDS) signature files from your config group to a local TFTP server, follow these steps:

Step 1 Choose **Configure > Controller Config Groups**.

Step 2 Select the check box to choose one or more config groups on the Config Groups page.

Step 3 Choose **Download IDS Signatures** from the Select a command drop-down list, and click **Go**.

Step 4 The Download IDS Signatures to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed. Choose **local machine** from the File is Located On field.

Step 5 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries field.

Step 6 Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout field.

Step 7 The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** to navigate to it. The controller uses this local filename as a base name and then adds _custom.sgi as a suffix.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried.

Step 8 Click **OK**.

Downloading Customized WebAuth

To download customized web authentication, follow these steps:

Step 1 Choose **Configure > Controller Config Groups**.

Step 2 Select the check box to choose one or more config groups on the Config Groups page.

Step 3 Choose **Download Customized WebAuth** from the Select a command drop-down list, and click **Go**.

Step 4 The Download Customized Web Auth Bundle to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed.

Step 5 Choose **local machine** from the File is Located On field.

CHAPTER 8

Configuring Devices

This chapter describes how to configure devices in the NCS database. It contains the following sections:

Configuring Controllers

This section describes how to configure controllers in the NCS database.

Choose **Configure > Controllers** to access the following:

- A summary of all controllers in the NCS database.
- The ability to add, remove, and reboot selected controllers.
- The ability to download software from the NCS server to selected controllers.
- The ability to save the current configuration to nonvolatile (flash) memory on selected controllers.
- The ability to view audit reports for selected controllers.

The controllers data table contains the following columns:

- Check box—Select the applicable controller.
- IP Address—Local network IP address of the controller management interface.
  - Click the title to sort the list items.

  - Click a list item to display parameters for that IP address. See the "Configuring Controllers Properties" section on page 8-24.
  - Click the icon to the right of the IP address to launch the controller web user interface in a new browser window.
- Device Name—Indicates the name of the controller. Click the **Controller Name** link to sort the list by controller name.
- Device Type—Click to sort by type. Based on the series, device types are grouped. For example:
  - WLC2100—21xx Series Wireless LAN Controllers
  - 2500—25xx Series Wireless LAN Controllers
  - 4400—44xx Series Wireless LAN Controllers
  - 5500—55xx Series Wireless LAN Controllers
  - 7500—75xx Series Wireless LAN Controllers
  - WiSM—WiSM (slot number, port number)
  - WiSM2—WiSM2 (slot number, port number)
- Location—Indicates the location of the controller.
- Software Version—The operating system release.version.dot.maintenance number of the code currently running on the controller.
- Mobility Group Name—Name of the mobility or WPS group.
- Reachability Status—Reachable or not reachable.

Note Reachability status is updated based on the last execution information of the Device Status background task. For updating the current status, choose **Administration > Background Tasks**, and choose **Execute Now** from the Select a command drop-down list.

- Audit Status
  - Not Available—No audit occurred on this switch.
  - Identical—No configuration differences were discovered.
  - Mismatch—Configuration differences were discovered.

  Click the **Audit Status** link to access the audit report. In the Audit Report page, choose **Audit Now** from the Select a command drop-down list to run a new audit for this controller. See the "Understanding the Controller Audit Report" section on page 8-3 for more information on audit reports.

Note Audit status is updated based on the last execution information of either the Configuration Sync background task or the Audit Now option located in the Controllers page. To get the current status, either choose **Administration > Background Tasks** and choose **Execute Now** or **Audit Now** from the Select a command drop-down list.

Note Use the Search feature to search for a specific controller. See the "Using the Search Feature" section on page 2-33 for more information.

This section contains the following topics:

Understanding the Controller Audit Report

The Controller Audit Report displays the following information depending on the type of audit selected in Administration > Settings > Audit and on which parameters the audit is performed:

- Applied template discrepancies (Template Based Audit only)
- Config group template discrepancies (Template Based Audit only)
- Total enforcements for config groups with background audit enabled (Template Based Audit only)
  - If the total enforcement count is greater than zero, this number appears as a link. Click the link to view a list of the enforcements made from NCS.
- Failed for config groups with background audit enabled (Template Based Audit only)
  - If the failed enforcement count is greater than zero, this number appears as a link. Click the link to view the failures returned from the device.
- Other NCS discrepancies

Note The controller audit report indicates if the audit was performed on all parameters or on a selected set of parameters.

Note See the "Configuring an Audit" section on page 15-53 for more in depth information on the two types of audits and how to manage specific parameters for the audit.

A current Controller Audit Report can be accessed in the Configure > Controllers page by clicking a value in the Audit Status column.

You can audit a controller by choosing **Audit Now** from the Select a command drop-down list in the Configure > Controllers page (See the "Using the Audit Now Feature" section on page 8-21 for more information) or by clicking **Audit Now** in the Controller Audit Report.

Adding Controllers

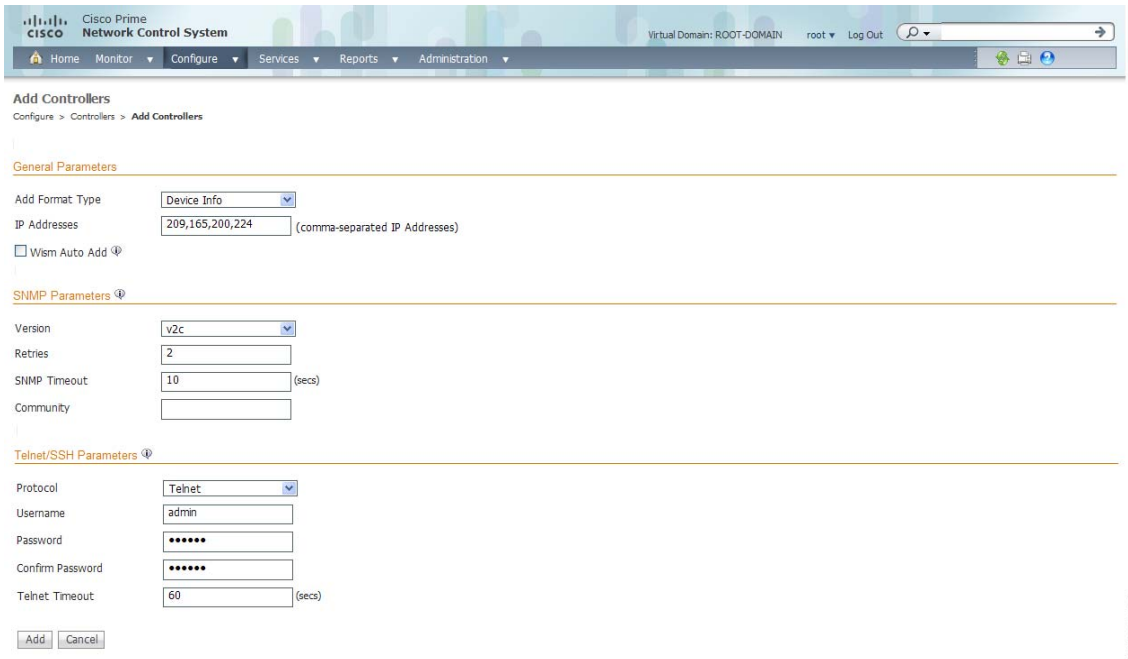
You can add controllers one at a time or in batches.

To add controllers, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 From the Select a command drop-down list, choose **Add Controllers**, and click **Go**. The Add Controller page appears (see Figure 8-1).

Figure 8-1 Add Controller Page



Step 3 Choose one of the following:

If you want to add one controller or use commas to separate multiple controllers, leave the Add Format Type drop-down list at Device Info.

If you want to add multiple controllers by importing a CSV file, choose **File** from the Add Format Type drop-down list. The CSV file allows you to generate your own import file and add the devices you want.

Note When a controller is removed from the system, the associated access points are not removed automatically and therefore remain in the system. These disassociated access points must be removed manually.

Note If you are adding a controller into the NCS across a GRE link using IPsec or a lower MTU link with multiple fragments, you might need to adjust the Maximum VarBinds per Get PDU and Maximum VarBinds per Set PDU. If it is set too high, the controller might fail to be added into the NCS. To adjust the Maximum VarBinds per Get PDU or Maximum VarBinds per Set PDU, do the following: Stop the NCS, choose **Administration > Settings > SNMP Settings**, and edit the Maximum VarBinds per Get PDU and Maximum VarBinds per Set PDU values to 50 or lower.

Note If you reduce the Maximum VarBinds per Get PDU or Maximum VarBinds per Set PDU value, applying the configurations to the device might fail.

Step 4 If you chose Device Info, enter the IP address of the controller you want to add. If you want to add multiple controllers, use a comma between the string of IP addresses.

Note If a partial byte boundary is used and the IP address appears to be broadcast (without regard to the partial byte boundary), there is a limitation on adding the controllers into the NCS. For example, 10.0.2.255/23 cannot be added but 10.0.2.254/23 can.

If you chose File, click **Browse** to find the location of the CSV file you want to import.

The first row of the CSV file is used to describe the columns included. The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory. The following example shows a sample CSV file.

```
ip_address,network_mask,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmp
v3_auth_password,snmpv3_privacy_type,snmpv3_privacy_password,snmp_retries,snmp_timeout,pro
tocol,telnet_username,telnet_password,enable_password,telnet_timeout
209.165.200.225,255.255.255.224,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
209.165.200.226,255.255.255.224,v2,public,,,,,3,10,,cisco,cisco,cisco,60
209.165.200.227,255.255.255.224,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
```

The CSV files can contain the following fields:

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password

- snmp_retries
- snmp_timeout
- protocol
- telnet_username
- telnet_password
- enable_password
- telnet_timeout

Step 5 Select the **Verify Telnet/SSH Credentials** check box if you want this controller to verify Telnet/SSH credentials. You might want to leave this unselected (or disabled) because of the substantial time it takes for discovery of the devices.

Note Enter SNMP parameters for the write access, if available. If you enter read-only access parameters, the controller is added but the NCS is unable to modify the configuration and the NCS can not be registered as a trap receiver on that Controller.

Step 6 Use the Version drop-down list to choose v1, v2, or v3.

Step 7 In the Retries text box, enter the number of times that attempts are made to discover the controller.

Step 8 Provide the client session timeout value in seconds. This determines the maximum amount of time allowed for a client before it is forced to reauthenticate.

Step 9 In the Community field, enter either public or private (for v1 and v2 only).

Note If you go back and later change the community mode, you must perform a refresh config for that controller.

Step 10 Choose None, HMAC-SHA, or HMAC-MD5 (for v3 only) for the authorization type.

Step 11 Enter the authorization password (for v3 only).

Step 12 Enter None, CBC-DES, or CFB-AES-128 (for v3 only) for the privacy type.

Step 13 Enter the privacy password (for v3 only).

Step 14 Enter the Telnet credentials information for the controller. If you chose the File option and added multiple controllers, the information applies to all specified controllers. If you added controllers from a CSV file, the username and password information is obtained from the CSV file.

Note The Telnet/SSH username must have sufficient privileges to execute commands in CLI templates.

The default username and password is admin.

Step 15 Enter the retries and timeout values. The default retries number is 3, and the default retry timeout is 1 minute.

Step 16 Click **OK**.

Note If you fail to add a device to the NCS, and if the error message 'Sparse table not supported' occurs, verify that the NCS and WLC versions are compatible and retry. For information on compatible versions, see the following URL: http://www.cisco.com/en/US/docs/wireless/controller/4400/tech_notes/Wireless_Software_Compatibility_Matrix.html.

Note When a controller is added to the NCS, the NCS acts as a TRAP receiver and the following traps are enabled on the controller: 802.11 Disassociation, 802.11 Deauthentication, and 802.11 Authenticated.

Note To update the credentials of multiple controllers in a bulk, choose **Bulk Update Controllers** from the Select a command drop-down list. The Bulk Update Controllers page appears. You can choose a CSV file. The CSV file contains a list of controllers to be updated, one controller per line. Each line is a comma separated list of controller attributes. The first line describes the attributes included. The IP address attribute is mandatory. For details, see the *Cisco Prime Network Control System Configuration Guide*.

Note After adding a controller, it is placed temporarily in the Monitor > Unknown Devices page while the NCS attempts to communicate with the controller that you have added. Once communication with the controller has been successful, the controller moves from the Monitor > Unknown Devices page to the Monitor > Controllers page. If the NCS is unable to successfully communicate with a controller, it remains in the Monitor > Unknown Devices and an error condition an error message is displayed. To access the Unknown Devices page, choose Configure > Unknown Devices.

Bulk Update of Controller Credentials

You can update multiple controllers credentials by importing a CSV file.

To update controller(s) information in bulk, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 From the Select a command drop-down list, choose **Bulk Update Controller**. The Bulk Update Controllers page appears.

Step 4 Enter the CSV filename in the Select CSV File text box or click **Browse** to locate the desired file.

Step 5 Click **Update and Sync**.

Sample CSV File for the Bulk Update of Controller Credentials

The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory. The following example shows a sample CSV file.

```
ip_address,network_mask,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmp
v3_auth_password,snmpv3_privacy_type,snmpv3_privacy_password,snmp_retries,snmp_timeout,pro
tocol,telnet_username,telnet_password,enable_password,telnet_timeout
209.165.200.225,255.255.255.224,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
209.165.200.226,255.255.255.224,v2,public,,,,,3,10,,cisco,cisco,cisco,60
209.165.200.227,255.255.255.224,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
```

The CSV files can contain the following fields:

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- protocol
- telnet_username
- telnet_password
- enable_password
- telnet_timeout

Removing Controllers from the NCS

To remove a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 From the Select a command drop-down list, choose **Remove Controllers**.

Step 4 Click **Go**.

Step 5 Click **OK** in the pop-up dialog box to confirm the deletion.

Note When a controller is removed from the system, the associated access points are not removed automatically and, therefore, remain in the system. These disassociated access points must be removed manually.

Rebooting Controllers

To reboot a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 From the Select a command drop-down list, choose **Reboot Controllers**.

Step 4 Click **Go**. The Reboot Controllers page appears (see Figure 8-2).

Note Save the current controller configuration prior to rebooting.

Figure 8-2 Reboot Controllers Page

Step 5 Select the Reboot Controller options that must be applied.

- Save Config to Flash—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.
- Reboot APs—Select the check box to enable a reboot of the access point after making any other updates.
- Swap AP Image—Indicates whether or not to reboot controllers and APs by swapping AP images. This could be either Yes or No.

Note Options are disabled unless the Reboot APs check box is selected.

Step 6 Click **OK** to reboot the controller with the optional configuration selected.

Downloading Software to Controllers

Both File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) are supported for uploading and downloading files to and from the NCS. In previous software releases, only TFTP was supported.

This section contains the following topics:

Downloading Software (FTP)

To download software to a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 From the Select a command drop-down list, choose **Download Software (FTP)**.

Step 4 Click **Go**.

Note Software can also be downloaded by choosing **Configure > Controllers >** *IPaddr* **> System > Commands > Upload/Download Commands > Download Software**.

The IP address of the controller and its current status appears in the Download Software to Controller page.

Step 5 Select the download type.

Note The pre-download option is displayed only when all selected controllers are using the Release 7.0.x.x or later.

- Now—Executes the download software operation immediately. If you select this option, proceed with Step 7.

  Note After the download is successful, reboot the controllers to enable the new software.

- Scheduled—Specify the scheduled download options.
  - Schedule download to controller—Select this check box to schedule download software to controller.
  - Pre-download software to APs—Select this check box to schedule the pre-download software to APs. The APs download the image and then reboot when the controller reboots.

    Note To see Image Predownload status per AP, enable the task in the Administration > Background Task > AP Image Predownload Task page, and run an AP Image Predownload report from the Report Launch Pad.

Step 6 If you selected the Scheduled option under Download type, enter the schedule details.

- Task Name—Enter a Scheduled Task Name to identify this scheduled software download task.
- Reboot Type—Indicates whether the reboot type is manual, automatic, or scheduled.

Note Reboot Type Automatic can be set when the only Download software to controller option is selected.

- Download date/time—Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists.
- Reboot date/time—This option appears only if you select the reboot type as "Scheduled". Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date to reboot the controller. Choose the time from the hours and minutes drop-down lists.

Note Schedule enough time (at least 30mins) between Download and Reboot so that all APs can complete the software pre-download.

Note If any one of the AP is in pre-download progress state at the time of scheduled reboot, the controller will not reboot. In such a case, wait for the pre-download to finish for all the APs and reboot the controller manually.

- Notification (Optional)—Enter the e-mail address of recipient to send notifications via e-mail.

Note To receive e-mail notifications, configure the NCS mail server in the Administration > Settings > Mail Server Configuration page.

Step 7 Enter the FTP credentials including username, password, and port.

Step 8 In the File is located on option, select either the **Local machine** or **FTP Server** radio button.

Note If you choose FTP Server, choose **Default Server** or **New** from the Server Name drop-down list.

Note The software files are uploaded to the FTP directory specified during the install.

Step 9 Specify the local filename or click **Browse** to navigate to the appropriate file.

Note If you chose FTP Server previously, specify the server filename.

Step 10 Click **Download**.

Note If the transfer times out for some reason, you can choose the FTP server option in the File is located on field; the server filename is populated and retried.

Downloading Software (TFTP)

To download software to a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 In the Select a command drop-down list, choose **Download Software (TFTP)**.

Step 4 Click **Go**.

Note Software can also be downloaded from Configure > Controllers > *IPaddr* > System > Commands > Upload/Download Commands > Download Software.

The IP address of the controller and its current status are displayed in the Download Software to Controller page.

Step 5 Select the download type.

Note The pre-download option is displayed only when all selected controllers are using the Release 7.0.x.x or later.

- Now—Executes the download software operation immediately. If you select this option, proceed with Step 7.

  Note After the download is successful, reboot the controllers to enable the new software.

- Scheduled—Specify the scheduled download options.
  - Download software to controller—Select this option to schedule download software to controller.
  - Pre-download software to APs—Select this option to schedule the pre-download software to APs. The APs download the image and then reboot when the controller reboots.

    Note To see Image Predownload status per AP, enable the task in the Administration > Background Task > AP Image Predownload Task page, and run an AP Image Predownload report from the Report Launch Pad.

Step 6 If you selected the Scheduled option under Download type, enter the schedule detail.

- Task Name—Enter a scheduled task name to identify this scheduled software download task.
- Reboot Type—Indicates whether the reboot type is manual, automatic, or scheduled.

Note Reboot Type Automatic can be set when only Download software to controller option is selected.

- Download date/time—Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists.
- Reboot date/time—This option appears only if you select the reboot type as "Scheduled". Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date to reboot the controller. Choose the time from the hours and minutes drop-down lists.

Note Schedule enough time (at least 30 minutes) between Download and Reboot so that all APs can complete the software pre-download.

Note If any one of the APs is in pre-download progress state at the time of scheduled reboot, the controller does not reboot. In such a case, wait for the pre-download to finish for all the APs and reboot the controller manually.

- Notification (Optional)—Enter the e-mail address of recipient to send notifications via e-mail.

Note To receive e-mail notifications, configure the NCS mail server in the Administration > Settings > Mail Server Configuration page.

Step 7 From the File is located on field, choose **Local machine** or **TFTP server**.

Note If you choose TFTP server, choose the Default Server or add a New server using the Server Name drop-down list.

Step 8 From the Maximum Retries field, enter the maximum number of tries the controller should attempt to download the software.

Step 9 In the Timeout field, enter the maximum amount of time (in seconds) before the controller times out while attempting to download the software.

Note The software files are uploaded to the TFTP directory specified during the install.

Step 10 Specify the local filename or click **Browse** to navigate to the appropriate file.

Note If you selected TFTP server previously, specify the server filename.

Step 11 Click **Download**.

Tip If the transfer times out for some reason, you can choose the TFTP server option in the File is located on field; the server filename is populated and retried.

Configuring *IPaddr* Upload Configuration/Logs from the Controller

To upload files from the controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP address column.

Step 3 From the left sidebar menu, choose **System > Commands**.

Step 4 Select the **FTP** or **TFTP** radio button.

Note Both File Transfer Protocol (FTP) and Trivial Transfer Protocol (TFTP) are supported for uploading and downloading files to and from the NCS. In previous software releases, only TFTP was supported.

Step 5 From the Upload/Download Commands drop-down list, choose **Upload File from Controller**.

Step 6 Click **Go** to access this page.

- FTP Credentials Information—Enter the FTP username, password, and port if you selected the FTP radio button previously.
- TFTP or FTP Server Information:
  - Server Name—From the drop-down list, choose **Default Server** or **New**.
  - IP Address—IP address of the controller. This is automatically populated if the default server is selected.
  - File Type—Select from configuration, event log, message log, trap log, crash file, signature files, or PAC.
  - Enter the Upload to File from /(root)/NCS-tftp/ or /(root)/NCS-ftp/ filename.
  - Select whether or not the NCS saves the information before backing up the configuration.

Note The NCS uses an integral TFTP and FTP server. This means that third-party TFTP and FTP servers cannot run on the same workstation as the NCS, because the NCS and the third-party servers use the same communication port.

Step 7 Click **OK**. The selected file is uploaded to your TFTP or FTP server and named what you entered in the File Name text box.

Downloading IDS Signatures

To download Intrusion Detection System (IDS) signature files to a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 From the Select a command drop-down list, choose **Download IDS Signatures**.

Step 4 Click **Go**.

Note IDS signature files can also be downloaded from Configure > Controllers > IPaddr > System > Commands > Upload/Download Commands > Download IDS Signatures.

In the Download IDS Signatures to Controller page, the controller IP address and its current status appears.

Step 5 Copy the signature file (*.sig) to the default directory on your TFTP server.

Step 6 In the File is located on option, select the **Local machine** radio button.

Note If you know the filename and path relative to the server root directory, you can also select the **TFTP server** radio button.

Step 7 In the Maximum Retries text box, enter the maximum number of tries the controller should attempt to download the signature file.

Step 8 In the Timeout text box, enter the maximum amount of time (in seconds) before the controller times out while attempting to download the signature file.

Note The signature files are uploaded to the c:\tftp directory.

Step 9 Specify the local filename or click **Browse** to navigate to the appropriate file. The controller uses this local filename as a base name and adds _custom.sgi as a suffix.

Note If you chose TFTP server previously, specify the server filename.

Step 10 Click **Download**.

Tip If the transfer times out for some reason, you can choose the TFTP server option in the File is located on field; the server filename is populated and retried.

Note The local machine option initiates a two-step operation. First, the local file is copied from the administrator workstation to the NCS own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the NCS server TFTP directory, and the downloaded web page now automatically populates the filename.

Downloading a Customized WebAuthentication Bundle to a Controller

To download customized web authentication bundle to a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 From the Select a command drop-down list, choose **Download Customized WebAuth**.

Step 4 Click **Go**.

Note A customized web authentication bundle can also be downloaded from Configure > Controllers > IPaddr > System > Commands > Upload/Download Commands > Download Customized Web Auth.

In the Download Customized WebAuth bundle to Controller page, the controller IP address and its current status appears.

Step 5 Select the **Local machine** radio button in the File is located on field.

Note If you know the filename and path relative to the server root directory, you can also select the **TFTP server** radio button.

Note For a local machine download, either .zip or .tar file options exists but the NCS does the conversion of .zip to .tar automatically. If you choose a TFTP server download, only .tar files are specified.

Step 6 In the Maximum Retries text box, enter the maximum number of tries the controller should attempt to download the file.

Step 7 In the Timeout text box, enter the maximum amount of time (in seconds) before the controller times out while attempting to download the file.

Note The NCS Server Files In field specifies where the NCS server files are located.

Step 8 Specify the local filename or click **Browse** to navigate to the appropriate file. The controller uses this local filename as a base name and adds _custom.sgi as a suffix.

Step 9 Click **Download**.

Tip If the transfer times out for some reason, you can select the **TFTP server** radio button in the File is located on field; the server filename is populated and retried.

Step 10 The local machine option initiates a two-step operation. First, the local file is copied from the administrator workstation to the NCS own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the NCS server TFTP directory, and the downloaded web page now automatically populates the filename.

Step 11 After completing the download, you are directed to a new page and are able to authenticate.

Downloading a Vendor Device Certificate

Each wireless device (controller, access point, and client) has its own device certificate. If you want to use your own vendor-specific device certificate, it must be downloaded to the controller.

To download a vendor device certificate to a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 You can download the certificate in one of two ways:

a. Select the check box(es) of the applicable controller(s).

b. From the Select a command drop-down list, choose **Download Vendor Device Certificate**.

c. Click **Go**.

-or-

a. Click the IP address of the desired controller.

b. Choose **System > Commands** from the left sidebar menu.

c. From the Upload/Download Commands drop-down list, choose **Download Vendor Device Certificate**.

d. Click **Go**.

Step 3 In the Certificate Password text box, enter the password used to protect the certificate.

Step 4 Reenter the password in the Confirm Password text box.

Step 5 In the File is located on field, select the **Local machine** or **TFTP server** radio button.

Note If the certificate is located on the TFTP server, enter the server filename. If it is located on the local machine, enter the local filename by clicking **Browse**.

Step 6 Enter the TFTP server name in the Server Name field. The default is the NCS server.

Step 7 Enter the server IP address.

Step 8 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 9 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 10 In the Local File Name text box, enter the directory path of the certificate.

Step 11 In the Server File Name text box, enter the name of the certificate.

Step 12 Click **Download**.

Downloading a Vendor CA Certificate

Controllers and access points have a certificate authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate might be used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific CA certificate, it must be downloaded to the controller.

To download a vendor CA certificate to the controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 You can download the certificate in one of two ways:

a. Select the check box(es) of the applicable controller(s).

b. From the Select a command drop-down list, choose **Download Vendor CA Certificate**.

c. Click **Go**.

-or-

a. Click the IP address of the desired controller.

b. Choose **System > Commands** from the left sidebar menu.

c. From the Upload/Download Commands drop-down list, choose **Download Vendor CA Certificate**.

d. Click **Go**.

Step 3 In the File is located on field, Select the **Local machine** or **TFTP server** radio button.

Note If the certificate is located on the TFTP server, enter the server file name. If it is located on the local machine, enter the local filename by clicking **Browse**.

Step 4 Enter the TFTP server name in the Server Name text box. The default is the NCS server.

Step 5 Enter the server IP address.

Step 6 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 7 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 8 In the Local File Name text box, enter the directory path of the certificate.

Step 9 In the Server File Name text box, enter the name of the certificate.

Step 10 Click **OK**.

Saving the Configuration to Flash

To save the configuration to flash memory, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box(es) for the applicable controller(s).

Step 3 From the Select a command drop-down list, choose **Save Config to Flash**.

Step 4 Click **Go**.

Refreshing the Configuration from the Controller

To refresh the configuration from the controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box(es) for the applicable controller(s).

Step 3 From the Select a command drop-down list, choose **Refresh Config from Controller**.

Step 4 Click **Go**.

Step 5 At the Configuration Change prompt, select the **Retain** or **Delete** radio button.

Step 6 Click **Go**.

Discovering Templates from the Controller

Prior to software Release 5.1, templates were detected when a controller was detected, and every configuration found on the NCS for a controller had an associated template. Now templates are not automatically detected with controller discovery, and you can specify which the NCS configurations you want to have associated templates.

Note The templates that are discovered do not retrieve management or local user passwords.

The following rules apply for template discovery:

- Template Discovery discovers templates that are not found in the NCS.
- Existing templates are not discovered.

To discover current templates, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box of the controller for which you want to discover templates.

Step 3 From the Select a command drop-down list, choose **Discover Templates from Controller**.

Step 4 Click **Go**. The Discover Templates page displays the number of discovered templates, each template type and each template name.

Note You can select the **Enabling this option will create association between discovered templates and the device listed above** check box so that discovered templates are associated to the configuration on the device and are shown as applied on that controller.

Note Template discovery refreshes configuration from the controller prior to discovering templates. Click **OK** in the warning dialog box to continue with the discovery.

Note For the TACACS+ Server templates, the configuration on the controller with same server IP address and port number but different server types are aggregated into one single template with the corresponding Server Types set on the Discovered Template. For the TACACS+ Server templates, the Admin Status on the discovered template reflects the value of Admin Status on the first configuration from the controller with same Server IP address and port number.

Updating Credentials in the NCS

To update SNMP/Telnet credential details in the NCS for multiple controllers, there is no configuration available. To perform this mass update, you need to go to each device and update the SNMP and Telnet credentials.

To update the SNMP/Telnet credentials, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box for each controller to which you want to update SNMP/Telenet credentials.

Step 3 From the Select a command drop-down list, choose **Update Credentials in NCS**. The Update Credentials in NCS page appears.

Step 4 Select the **SNMP Parameters** check box and configure the following parameters:

Note SNMP write access parameters are needed for modifying controller configuration. With read-only access parameters, configuration can only be displayed.

- Version—Choose from v1, v2, or v3.
- Retries—Indicates the number of controller discovery attempts.
- Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The valid range is 2 to 90 seconds. The default is 2 seconds.
- Community—Public or Private.
- Verify SNMP Credentials—Select this check box to verify SNMP credentials.

Step 5 Select the **Telnet/SSH Parameters** check box and configure the following parameters:

- User Name—Enter the username.
- Password/Confirm Password—Enter and confirm the password.
- Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The valid range is 2 to 90 seconds. The default is 60 seconds.

Viewing Templates Applied to a Controller

You can view all templates currently applied to a specific controller.

Note Only templates applied in this partition are displayed.

To view applied templates, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box for the applicable controller.

Step 3 From the Select a command drop-down list, choose **Templates Applied to a Controller**.

Step 4 Click **Go**. The Templates Applied to a Controller page displays each applied template name, template type, the date the template was last saved, and the date the template was last applied.

Note Click the template name link to view the template details. See the "Using Templates" section on page 10-1 for more information.

Using the Audit Now Feature

You can audit a controller by choosing **Audit Now** from the Select a command drop-down list in the Configure > Controllers page or by choosing **Audit Now** directly from the Select a command drop-down list.

Note A current Controller Audit Report can be accessed in the Configure > Controllers page by clicking a value in the Audit Status column.

To audit a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box for the applicable controller.

Step 3 From the Select a command drop-down list, choose **Audit Now**.

Step 4 Click **Go**.

Step 5 Click **OK** in the pop-up dialog box if you want to remove the template associations from configuration objects in the database as well as template associations for this controller from associated config groups (Template based audit only).

The Audit Report displays:

- Device Name
- Time of Audit
- Audit Status
- Applied and Config Group Template Discrepancies information including the following:
  - Template type (template name)
  - Template application method
  - Audit status (For example, mismatch, identical)
  - Template attribute
  - Value in NCS
  - Value in Controller
- Other NCS Discrepancies including the following:
  - Configuration type (name)
  - Audit Status (For example, mismatch, identical)
  - Attribute
  - Value in NCS
  - Value in Controller
- Total enforcements for config groups with background audit enabled—If discrepancies are found during the audit in regards to the config groups enabled for background audit and if the enforcement is enabled, this section lists the enforcements made during the controller audit. See the "Configuring Config Groups" section on page 8-223 for more information on enabling the background audit.
- Failed Enforcements for Config Groups with background audit enabled—Click the link to view a list of failure details (including the reason for the failure) returned by the device. See the "Configuring Config Groups" section on page 8-223 for more information on enabling the background audit (ConfigAuditSet).
- Restore the NCS Values to Controller or Refresh Config from Controller—If there are config differences found as a result of the audit, you can either click **Restore NCS Values to controller** or **Refresh Config from controller** to bring the NCS configuration in sync with the controller.
  - Choose **Restore NCS Values to Controller** to push the discrepancies to the device.
  - Choose **Refresh config from controller** to pick up the device for this configuration from the device.

Note Templates are not refreshed as a result of clicking Refresh Config from Controller.

Viewing the Latest Network Audit Report

The Network Audit Report shows the time of the audit, the IP address of the selected controller, and the synchronization status.

Note This method shows the report from the network audit task and not an on-demand audit per controller.

To view the latest network audit report for the selected controllers, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box for the applicable controller.

Step 3 From the Select a command drop-down list, choose **View Latest Network Configuration Audit Report**.

Step 4 Click **Go**.

The Audit Summary displays the time of the audit, the IP address of the selected controller, and the audit status. The Audit Details display the config differences, if applicable.

Note Use the General and Schedule tabs to revise Audit Report parameters.

Command Buttons

- Save—Click to save changes made to the current parameters.
- Save and Run—Click to save the changes to the current parameters and run the report.
- Run Now—Click to run the audit report based on existing parameters.
- Export Now—Click to export the report results. The supported export formats is PDF and CSV.
- Cancel—Click to cancel any changes made to the existing parameters.

Note From the All Controllers page, click the Audit Status column value to view the latest audit details page for the selected controller. This method has similar information as the Network Audit report on the Reports menu, but this report is interactive and per controller.

Note To run an on-demand audit report, choose which controller you want to run the report on and choose **Audit Now** from the Select a command drop-down list. If you run an on-demand audit report and configuration differences are detected, you are given the option to retain the existing controller or the NCS values.

Configuring Existing Controllers

This section contains the following topics:

Configuring Controllers Properties

To configure the properties for current controllers, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Properties > Settings**. The following parameters appear:

- General Parameters:
  - Name—Name assigned to the controller.
  - Type—Controller type.
  - Restore on Cold Start Trap—Select to enable a restore on a cold start trap.
  - Auto Refresh on Save Config Trap—Select to enable an automatic refresh on a Save Config trap.
  - Trap Destination Port—Read-only.
  - Software Version—Read-only.
  - Location—Location of the controller.
  - Contact—The contact person for this controller.
  - Most Recent Backup—The date and time of the most recent backup.
  - Save Before Backup—Select to enable a save before backup.
- SNMP Parameters:

Note SNMP write access parameters are needed for modifying controller configuration. With read-only access parameters, configuration can only be displayed.

- Version—Choose from v1, v2, or v3.
- Retries—Indicates the number of controller discovery attempts.
- Timeout (seconds)—Client Session timeout. Sets the maximum amount of time allowed a client before it is forced to reauthenticate.
- Community—Public or Private.
- Access Mode—Read Write

Note Community settings only apply to v1 and v2.

- User Name—Enter a username.
- Auth. Type—Choose an authentication type from the drop-down list or choose **None**.
- Auth. Password—Enter an authentication password.
- Privacy Type—Choose a privacy type from the drop-down list or choose **None**.
- Privacy Password—Enter a privacy password.

Note User Name, Auth. Type, Auth. Password, Privacy Type, and Privacy Password only display for v3.

- Telnet/SSH Parameters:
  - User Name—Enter the username. (Default username is admin.)

Note The Telnet/SSH username must have sufficient privileges to execute commands in CLI templates.

  - Password/Confirm Password—Enter and confirm the password. (Default password is admin.)
  - Retries—Indicate the number of allowed retry attempts. The default is three.
  - Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The default is 60 seconds.

Note Default values are used if the Telnet/SSH parameters are left blank.

Step 4 If you made changes to this controller properties, click **Save** to confirm the changes, **Reset** to return to the previous or default settings, or **Cancel** to return to the Configure > Controllers page without making any changes to these settings.

Configuring Controller System Parameters

This section describes how to configure the controller system parameters and contains the following topics:

Managing General System Properties for Controllers

To view the general system parameters for a current controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > General**. The following parameters appear:

- 802.3x Flow Control Mode—Disable or enable. See the "802.3x Flow Control" section on page 8-30 for more information.
- 802.3 Bridging—Disable or enable. See the "Configuring 802.3 Bridging" section on page 8-30 for more information.
- Web Radius Authentication—Choose PAP, CHAP, or MD5-CHAP.
  - PAP—Password Authentication Protocol. Authentication method where user information (username and password) is transmitted in clear text.
  - CHAP—Challenge Handshake Authentication Protocol. Authentication method where user information is encrypted for transmission.
  - MD5-CHAP—Message Digest 5 Challenge Handshake Authentication Protocol. With MD5, passwords are hashed using the Message Digest 5 algorithm.
- AP Primary Discovery Timeout—Enter a value between 30 and 3600 seconds.

  The access point maintains a list of backup controllers and periodically sends primary discovery requests to each entry in the list. When configured, the primary discovery request timer specifies the amount of time that a controller has to respond to the discovery request of the access point before the access point assumes that the controller cannot be joined and waits for a discovery response from the next controller in the list.

- CAPWAP Transport Mode—Layer 3 or Layer 2. See the "Lightweight Access Point Protocol Transport Mode" section on page 8-30 for more information.
- Current LWAPP Operating Mode—Automatically populated.
- Broadcast Forwarding—Disable or enable.
- LAG Mode—Choose **Disable** if you want to disable LAG.

  Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. It bundles all of the controller distribution system ports into a single 802.3ad port channel, thereby reducing the number of IP addresses needed to configure the ports on your controller. When LAG is enabled, the system dynamically manages port redundancy and load balances access points transparently to the user.

  Note LAG is disabled by default on the Cisco 5500 and 4400 series controllers but enabled by default on the Cisco WiSM and the controller in the Catalyst 3750G Integrated Wireless LAN Controller Switch.

  See the "Link Aggregation" section on page 8-32 for more information.
- Ethernet Multicast Support
  - Disable—Select to disable multicast support on the controller.
  - Unicast—Select if the controller, upon receiving a multicast packet, forwards the packets to all the associated access points.

    Note FlexConnect supports only unicast mode.

  - Multicast—Select to enable multicast support on the controller.
- Aggressive Load Balancing—Disable or enable. See the "Aggressive Load Balancing" section on page 8-31 for more information on load balancing.
- Peer to Peer Blocking Mode
  - Disable—Same-subnet clients communicate through the controller.
  - Enable—Same-subnet clients communicate through a higher-level router.
- Over Air Provision AP Mode—Disable or enable.

  Over-the-air provisioning (OTAP) is supported by Cisco 5500 and 4400 series controllers. If this feature is enabled on the controller, all associated access points transmit wireless CAPWAP or LWAPP neighbor messages, and new access points receive the controller IP address from these messages. This feature is disabled by default and should remain disabled when all access points are installed.

  Note Disabling OTAP on the controller does not disable it on the access point. OTAP cannot be disabled on the access point.

  Note You can find additional information about OTAP at the following URL: http://www.ciscosystems.com/en/US/products/ps6366/products_tech_note09186a008093d74a.shtml

- AP Fallback—Disable or enable.

Note Enabling AP Fallback causes an access point which lost a primary controller connection to automatically return to service when the primary controller returns.

- AP Failover Priority—Disable or enable.

Note To configure failover priority settings for access points, you must first enable the AP Failover Priority feature. See the "AP Failover Priority" section on page 8-29 for more information.

- AppleTalk Bridging—Disable or enable.
- Fast SSID change—Disable or enable.

  When fast SSID changing is enabled, the controller allows clients to move between SSIDs. When the client sends a new association for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID. When fast SSID changing is disabled, the controller enforces a delay before clients are allowed to move to a new SSID.

Note If enabled, the client connects instantly to the controller between SSIDs without having appreciable loss of connectivity.

- Master Controller Mode—Disable or enable.

Note Because the master controller is normally not used in a deployed network, the master controller setting is automatically disabled upon reboot or OS code upgrade.

- Wireless Management—Disable or enable. See the "Wireless Management" section on page 8-32 for more information.
- Symmetric Tunneling Mode
- ACL Counters—Disable or enable. The number of hits are displayed in the ACL Rule page. See the "Configuring Access Control Lists" section on page 8-102 or the "Configuring IPaddr > Access Control List > listname Rules" section on page 8-102 for more information.
- Multicast Mobility Mode—Disable or enable. See the "Setting the Mobility Scalability Parameters" section on page 8-53 for more information.
- Default Mobility Domain Name—Enter domain name.
- Mobility Anchor Group Keep Alive Interval—Enter the amount of delay time allowed between tries for a client attempting to join another access point. See the "Mobility Anchor Group Keep Alive Interval" section on page 8-32 for more information.

Tip When you hover your mouse cursor over the parameter text box, the valid range for that field appears.

- Mobility Anchor Group Keep Alive Retries—Enter number of allowable retries.

Tip When you hover your mouse cursor over the parameter text box, the valid range for that field appears.

- RF Network Name—Enter network name.
- User Idle Timeout (seconds)—Enter timeout in seconds.
- ARP Timeout (seconds)—Enter timeout in seconds.

This section contains the following topics:

AP Failover Priority

When a controller fails, the backup controller configured for the access point suddenly receives a number of Discovery and Join requests. If the controller becomes overloaded, it might reject some of the access points.

By assigning failover priority to an access point, you have some control over which access points are rejected. When the backup controller is overloaded, join requests of access points configured with a higher priority levels take precedence over lower-priority access points.

To configure failover priority settings for access points, you must first enable the AP Failover Priority feature.

To enable the AP Failover Priority feature, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > General**.

Step 4 From the AP Failover Priority drop-down list, choose **Enabled**.

To configure an access point failover priority, follow these steps:

Step 1 Choose **Configure > Access Points >** *AP Name*.

Step 2 From the AP Failover Priority drop-down list, choose the applicable priority (**Low**, **Medium**, **High, Critical**).

Note The default priority is Low.

Configuring 802.3 Bridging

The controller supports 802.3 frames and applications that use them, such as those typically used for cash registers and cash register servers. However, to make these applications work with the controller, the 802.3 frames must be bridged on the controller.

Support for raw 802.3 frames allows the controller to bridge non-IP frames for applications not running over IP. Only this raw 802.3 frame format is currently supported.

To configure 802.3 bridging using the NCS release 4.1 or later, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 Choose **System > General** to access the General page.

Step 4 From the 802.3 Bridging drop-down list, choose **Enable** to enable 802.3 bridging on your controller or **Disable** to disable this feature. The default value is Disable.

Step 5 Click **Save** to confirm your changes.

802.3x Flow Control

Flow control is a technique for ensuring that a transmitting entity, such as a modem, does not overwhelm a receiving entity with data. When the buffers on the receiving device are full, a message is sent to the sending device to suspend the transmission until the data in the buffers has been processed.

By default, flow control is disabled. You can only enable a Cisco switch to receive PAUSE frames but not to send them.

Lightweight Access Point Protocol Transport Mode

Lightweight Access Point Protocol transport mode indicates the communications layer between controllers and access points. Selections are Layer 2 or Layer 3.

To convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 lightweight access point transport mode using the NCS user interface, follow these steps:

Note Cisco IOS-based lightweight access points do not support Layer 2 lightweight access point mode. These access points can only be run with Layer 3.

Note This procedure causes your access points to go offline until the controller reboots and the associated access points reassociate to the controller.

Step 1 Make sure that all controllers and access points are on the same subnet.

Note You must configure the controllers and associated access points to operate in Layer 2 mode before completing the conversion.

Step 2 Log in to the NCS user interface. Then follow these steps to change the lightweight access point transport mode from Layer 3 to Layer 2:

a. Choose **Configure > Controllers**.

b. Click the IP address of the applicable controller.

c. Choose **System > General** to access the General page.

d. Change lightweight access point transport mode to Layer2 and click **Save**.

e. If the NCS displays the following message, click **OK**:

```
Please reboot the system for the CAPWAP Mode change to take effect.
```

Step 3 To restart the NCS, follow these steps:

a. Choose **System > Commands**.

b. From the Administrative Commands drop-down list, choose **Save Config To Flash**, and click **Go** to save the changed configuration to the controller.

c. Click **OK** to continue.

d. From the Administrative Commands drop-down list, choose **Reboot**, and click **Go** to reboot the controller.

e. Click **OK** to confirm the save and reboot.

Step 4 After the controller reboots, follow these steps to verify that the CAPWAP transport mode is now Layer 2:

a. Choose **Configure> Controllers**.

b. Click the IP address of the applicable controller.

c. Verify that the current CAPWAP transport mode is Layer2 from the general drop-down list.

You have completed the CAPWAP transport mode conversion from Layer 3 to Layer 2. The operating system software now controls all communications between controllers and access points on the same subnet.

Aggressive Load Balancing

In routing, load balancing refers to the capability of a router to distribute traffic over all its network ports that are the same distance from the destination address. Good load-balancing algorithms use both line speed and reliability information. Load balancing increases the use of network segments, thus increasing effective network bandwidth.

Aggressive load balancing actively balances the load between the mobile clients and their associated access points.

Link Aggregation

Link aggregation allows you to reduce the number of IP addresses needed to configure the ports on your controller by grouping all the physical ports and creating a link aggregation group (LAG). In a 4402 model, two ports are combined to form a LAG whereas in a 4404 model, all four ports are combined to form a LAG.

If LAG is enabled on a controller, the following configuration changes occur:

- Any dynamic interfaces that you have created are deleted. This is done to prevent configuration inconsistencies in the interface database.
- Interfaces cannot be created with the "Dynamic AP Manager" flag set.

Note You cannot create more than one LAG on a controller.

The advantages of creating a LAG include the following:

- Assurance that, if one of the links goes down, the traffic is moved to the other links in the LAG. As long as one of the physical ports is working, the system remains functional.
- No need to configure separate backup ports for each interface.
- Multiple AP-manager interfaces are not required because only one logical port is visible to the application.

Note When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect.

Tip When you hover your mouse cursor over the parameter text box, the valid range for that field appears.

Wireless Management

Because of IPsec operation, management via wireless is only available to operators logging in across WPA, Static WEP, or VPN Pass Through WLANs. Wireless management is not available to clients attempting to log in via an IPsec WLAN.

Mobility Anchor Group Keep Alive Interval

Indicate the delay between tries for clients attempting to join another access point. This decreases the time it takes for a client to join another access point following a controller failure because the failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

Tip When you hover your mouse cursor over the parameter text box, the valid range for that field appears.

Configuring Controller System Commands

To view the System Command parameters for current controllers, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Commands**. The following parameters appear:

- Administrative
  - Reboot—This command enables you to confirm the restart of your controller after saving your configuration changes. Open and confirm a new session and log into the controller to avoid loosing a system connection.
  - Save Config to Flash—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.
  - Reset to Factory Default—Choose this command to return the controller to its original settings. See the "Restoring Factory Defaults" section on page 8-34 for more information.
  - Ping From Controller—Send a ping to a network element. This pop-up dialog box allows you to tell the controller to send a ping request to a specified IP address. This is useful for determining if there is connectivity between the controller and a particular IP station. If you click **OK**, three pings are sent and the results of the ping are displayed in the pop-up. If a reply to the ping is not received, it shows No Reply Received from IP xxx.xxx.xxx.xxx, otherwise it shows Reply received from IP xxx.xxx.xxx.xxx: (send count =3, receive count = n).
- Configuration
  - Audit Config—See the "Viewing the Latest Network Audit Report" section on page 8-23.
  - Refresh Config From Controller—See the "Refreshing the Configuration from the Controller" section on page 8-19.
  - Restore Config To Controller—Choose this command to restore the configuration from the NCS database to the controller.
  - Set System Time—See the "Setting the Controller Time and Date" section on page 8-35.
- Upload/Download Commands

Note Select the **FTP** or **TFTP** radio button. Both File Transfer Protocol (FTP) and Trivial Transfer Protocol (TFTP) are supported for uploading and downloading files to and from the NCS. In previous software releases, only TFTP was supported.

  - Upload File from Controller—See the "Uploading Configuration/Logs from Controllers" section on page 8-35.
  - Download Config—See the "Downloading Configurations to Controllers" section on page 8-36.
  - Download Software—Choose this command to download software to the selected controller or all controllers in the selected groups after you have a configuration group established. See the "Downloading Software to a Controller" section on page 8-36.
  - Download Web Auth Cert—Choose this command to access the Download Web Auth Certificate to Controller page. See the "Downloading a Web Admin Certificate to a Controller" section on page 8-37.
  - Download Web Admin Cert—Choose this command to access the Download Web Admin Certificate to Controller page. See the "Downloading a Web Admin Certificate to a Controller" section on page 8-37.

  - Download IDS Signatures—Choose this command to download customized signatures to the standard signature file currently on the controller. See the "Downloading Signature Files" section on page 8-111 for more information.
  - Download Customized Web Auth—Choose this command to download a customized Web authentication page to the controller. A customized web page is created to establish a username and password for user web access. See the "Downloading a Customized WebAuthentication Bundle to a Controller" section on page 8-16.
  - Download Vendor Device Certificate—Choose this command to download your own vendor-specific device certificate to the controller to replace the current wireless device certificate. See the "Downloading a Vendor Device Certificate" section on page 8-17.
  - Download Vendor CA Certificate—Choose this command to download your own vendor-specific certificate authority (CA) to the controller to replace the current CA. See the "Downloading a Vendor CA Certificate" section on page 8-18.
- RRM Commands
  - RRM 802.11a/n Reset—Resets Remote Radio Management for 802.11a/n Cisco Radios.
  - 802.11b/g/n Reset—Resets Remote Radio Management for 802.11b/g/n Cisco Radios.
  - 802.11a/n Channel Update—Updates access point dynamic channel algorithm for 802.11a/n Cisco Radios.
  - 802.11b/g/n Channel Update—Updates access point dynamic channel algorithm for 802.11b/g/n Cisco Radios.
  - 802.11a/n Power Update—Updates access point dynamic transmit power algorithm for 802.11a/n Cisco Radios.
  - 802.11b/g/n Power Update—Updates access point dynamic transmit power algorithm for 802.11b/g/n Cisco Radios.

Restoring Factory Defaults

Choose **Configure > Controllers**, and click an IP address in the IP Address column. From the left sidebar menu, choose **System > Commands**, and from the Administrative Commands drop-down list, choose **Reset to Factory Default**, and click **Go** to access this page.

This command enables you to reset the controller configuration to the factory default. This overwrites all applied and saved configuration parameters. You are prompted for confirmation to reinitialize your controller.

All configuration data files are deleted, and upon reboot, the controller is restored to its original non-configured state. This removes all IP configuration, and you need a serial connection to restore its base configuration.

Note After confirming configuration removal, you must reboot the controller and select the **Reboot Without Saving** option.

Setting the Controller Time and Date

Choose **Configure > Controllers**, and click an IP address under the IP Address column. From the left sidebar menu, choose **System > Commands**, and from the Configuration Commands drop-down list choose **Set System Time**, and click **Go** to access this page.

Use this command to manually set the current time and date on the controller. To use a Network Time Server to set or refresh the current time, see the "Configuring an NTP Server Template" section on page 10-10 page. The following parameters appear:

- Current Time—Shows the time currently being used by the system.
- Month/Day/Year—Choose the month/day/year from the drop-down list.
- Hour/Minutes/Seconds—Choose the hour/minutes/seconds from the drop-down list.
- Delta (hours)—Enter the positive or negative hour offset from GMT (Greenwich Mean Time).
- Delta (minutes)—Enter the positive or negative minute offset from GMT.
- Daylight Savings—Select to enable Daylight Savings Time.

Command Buttons

- Set Date and Time
- Set Time Zone
- Cancel

Uploading Configuration/Logs from Controllers

To upload files from the controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

Step 3 From the left sidebar menu, choose **System > Commands**.

Step 4 From the Upload/Download Commands drop-down list, choose **Upload File from Controller**.

Step 5 Click **Go** to access this page.

Use this command to upload files from your controller to a local TFTP (Trivial File Transfer Protocol) server. The following fields appear:

- IP Address—IP address of the controller.
- Status—Upload NOT_INITIATED, or other state.
- Enter the TFTP server name, or New and the new TFTP server name.
- Verify and/or enter the IP Address of the TFTP server.
- Select the file type—Configuration file, Event Log, Message Log, Trap Log, Crash File.
- Enter the Upload to File from /(root)/NCS-tftp/ filename.
- Choose whether or not the NCS saves before backing up the configuration.

Step 6 Click **OK**. The selected file is uploaded to your TFTP server and named what you entered in the File Name text box.

Note The NCS uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as the NCS, because the Cisco NCS and the third-party TFTP servers use the same communication port.

Downloading Configurations to Controllers

To download configuration files, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

Step 3 From the left sidebar menu, choose **System > Commands**.

Step 4 From the Upload/Download Commands drop-down list, choose **Download Config**.

Step 5 Click **Go** to access this page.

Use this command to download and install a configuration file to your controller from a local TFTP (Trivial File Transfer Protocol) server. The following parameters appear:

Note The NCS uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as the NCS, because the NCS and the third-party TFTP servers use the same communication port.

- IP Address—IP address of the controller.
- Status—Status of the certificate, for example, NOT_INITIATED.

TFTP Servers

- Server Name—Choose Default Server or **New** from the drop-down list. When you choose New, type in the IP address.
- Server Address—IP address of the server.
- Maximum Retries—How many times to retry if the download fails.
- Timeout—How long to allow between retries.
- File Name—Enter or choose the filename to download by clicking **Browse**.

Downloading Software to a Controller

To download software, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

Step 3 From the left sidebar menu, choose **System > Commands**.

Step 4 From the Upload/Download Commands drop-down list, choose **Download Software**.

Step 5 Click **Go** to access this page.

Use this command to download and install a new Operating System software to your controller from a local TFTP (Trivial File Transfer Protocol) server.

Note The NCS uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as the NCS, because the NCS and the third-party TFTP servers use the same communication port.

- IP Address—IP address of the controller to receive the software.
- Current Software Version—The software version currently running on the controller.
- Status—Status of the software, for example, NOT_INITIATED.
- TFTP Server on Cisco NCS System—Select the check box enable the built-in Cisco NCS TFTP server.
- Server IP Address—Indicates the IP address of the TFTP server to send the software to the controller when you have disabled the built-in NCS TFTP server.
- Maximum Retries—Maximum number of unsuccessful attempts before the download is abandoned.
- Timeout—Maximum number of seconds before the download is abandoned.
- File Name—Enter or select the filename to download by clicking **Browse**.

Downloading a Web Admin Certificate to a Controller

To download a Web Admin Certificate, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

Step 3 From the left sidebar menu, choose **System > Commands**.

Step 4 From the Upload/Download Commands drop-down list, choose **Download WEB Admin Cert**.

Step 5 Click **Go** to access this page.

This page enables you to download a web administration certificate to the controller. The following parameters appear:

Caution Each certificate has a variable-length embedded RSA Key. The RSA key length varies from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you are obtaining a new certificate from a certificate authority (such as the Microsoft CA), Make sure the RSA key embedded in the certificate is at least 768 Bits.

- IP Address—IP address of the controller to receive the certificate.
- Status—Status of the certificate, for example, NOT_INITIATED.

TFTP Servers

- Server Name—Use the drop-down list to choose the **Default Server** or **New**. When you select New, type in the IP address.
- Server Address—IP address of the server.
- Maximum Retries—Maximum number of times each download operation can be attempted.
- Timeout (seconds)—The amount of time allowed for each download operation.
- File Name—File name of the certificate.
- Password—Password to access the certificate.

Downloading IDS Signatures

To download a IDS Signature, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

Step 3 From the left sidebar menu, choose **System > Commands**.

Step 4 From the Upload/Download Commands drop-down list, choose **Download IDS Signatures**.

Step 5 Click **Go** to access this page.

Use this command to download IDS (Intrusion Detection System) signature files from your controller to a local TFTP (Trivial File Transfer Protocol) server. The following parameters appear:

- IP Address—IP address of the controller.
- Status—Download NOT_INITIATED, TRANSFER_SUCCESSFUL or other state.

Downloading a Customized Web Auth Bundle to a Controller

To download a customized web authentication page to the controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

Step 3 From the left sidebar menu, choose **System > Commands**.

Step 4 From the Upload/Download Commands drop-down list, choose **Download Customized Web Auth**.

The following parameters appear:

- IP Address—IP address of the controller to receive the bundle.
- Status—State of download: NOT_INITIATED, TRANSFER_SUCCESSFUL, TRANSFER_FAILED, NOT_RESPONDING.

Before downloading the customized Web authentication bundle, follow these steps:

Step 1 Click the indicated link to download the example login.tar bundle file from the server.

The link is the highlighted word “here” near the bottom of the page.

Step 2 Edit the login.html file and save it as a .tar or .zip file.

Step 3 Download the .tar or .zip file to the controller.

The file contains the pages and image files required for the web authentication display.

Note The controller accepts a .tar or .zip file of up to 1 MB in size. The 1 MB limit includes the total size of uncompressed files in the bundle.

TFTP Servers

To set up one or more TFTP servers, configure the following parameters:

- File is located on—Choose **Local machine** or **TFTP server**. The default is local machine (the NCS internal server).
- Server Name—Use the drop-down list to choose one of the following:
  - **New**—Set up a new server. Enter the server name and IP address in the text boxes provided.
  - **Default Server**—The server name (editable) and IP address (read-only) are automatically added.
- Server IP Address—IP address of the server.
- Maximum Retries—Maximum number of unsuccessful attempts before the download is abandoned.
- Timeout—Maximum number of seconds before the download is abandoned.
- NCS Server Files In—C:\tftp or other specified file directory on the local machine.
- Local File Name—Filename of the Web authentication bundle on the local machine. Click **Browse** to locate the file.
- Server File Name—Filename on a remote TFTP server.

When completed, these fields and settings are repopulated in the page and do not need to be entered again.

Command Buttons

- OK—The file is downloaded from the local machine or TFTP server with the name shown in the File Name text box.
- Cancel

Configuring Controller System Interfaces

This section describes how to configure controller system interfaces and contains the following topics:

- Configuring Wired Guest Access, page 8-47

To view existing interfaces, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Interfaces**. The following parameters appear:

- Check box—Select the dynamic interface for deletion. Choose **Delete Dynamic Interfaces** from the Select a command drop-down list.
- Interface Name—User-defined name for this interface (For example, Management, Service-Port, Virtual).
- VLAN Identifier—VLAN identifier between 0 (untagged) and 4096, or N/A.
- Quarantine—Select the check box if the interface has a quarantine VLAN ID configured on it.
- IP Address—IP address of this interface.
- Interface Type—Static (Management, AP-Manager, Service-Port, and Virtual interfaces) or Dynamic (operator-defined interfaces).
- AP Management Status—Displays the status of AP Management interfaces. The parameters include Enabled, Disabled, and N/A.

Adding an Interface

To add an interface, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Interfaces**.

Step 4 From the Select a command drop-down list, choose **Add Interface**.

Step 5 Enter the necessary parameters:

- Interface Name—User-defined name for this interface (Management, Service-Port, Virtual, and VLAN n).
- Wired Interface—Select the check box to mark the interface as wired.
- Interface Address
  - VLAN Identifier—1 through 4096, or 0 = untagged.
  - Quarantine—Enable/disable to quarantine a VLAN. Select the check box to enable.
  - IP Address—IP address of the interface.
  - Gateway—Gateway address of the interface.
- Physical Information
  - Port Number—The port that is used by the interface.
  - Primary Port Number (active)—The port that is currently used by the interface.
  - Secondary Port Number—The port that is used by the interface when the primary port is down.

Note Primary and secondary port numbers are only present in Cisco 4400 Series Wireless LAN controllers.

Note The secondary port is used when the primary port shuts down. When the primary port is reactivated, the Cisco 4400 Series Wireless LAN controller transfers the interfaces back to the primary port.

  - AP Management—Select to enable access point management.
- DHCP Information
  - Primary DHCP Server—IP address of the primary DHCP server.
  - Secondary DHCP Server—IP address of the secondary DHCP server.
- Access Control List—User-defined ACL name (or none).

Viewing Current Interface Details

To view details for a current interface, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Interfaces**.

Step 4 Select the Interface Name for the applicable interface. The Interface Details page opens.

Step 5 View or edit the following interface parameters:

Note Changing the Interface parameters causes the WLANs to be temporarily disabled and thus might result in loss of connectivity for some clients.

- Interface Address
  - VLAN Identifier—1 through 4096, or 0 = untagged.
  - Guest LAN
  - Quarantine—Enable/disable to quarantine a VLAN. Select the check box to enable.
  - IP Address—IP address of the interface.
  - Gateway—Gateway address of the interface.
- Physical Information
  - Primary Port Number (active)—The port that is currently used by the interface.
  - Secondary Port Number—The port that is used by the interface when the primary port is down.

Note Primary and secondary port numbers are only present in Cisco 4400 Series Wireless LAN Controllers.

Note The secondary port is used when the primary port shuts down. When the primary port is reactivated, the Cisco 4400 Series Wireless LAN Controller transfers the interfaces back to the primary port.

  - AP Management—Select to enable access point management.
- DHCP Information
  - Primary DHCP Server—IP address of the primary DHCP server.
  - Secondary DHCP Server—IP address of the secondary DHCP server.
- Access Control List
  - ACL Name—User-defined name of the access control list (or none).

Step 6 Click **Save** to confirm any changes made. Click **Audit** to audit the device values.

Deleting a Dynamic Interface

To delete a dynamic interface, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Interfaces**.

Step 4 Select the check box of the dynamic interface that you want to delete.

Step 5 From the Select a command drop-down list, choose **Delete Dynamic Interfaces**.

Step 6 Click **OK** to confirm the deletion.

Note The dynamic interface cannot be deleted if it has been assigned to interface group.

Configuring Controller System Interface Groups

This section describes how to configure controller system interface groups and contains the following topics:

Adding an Interface Group

To add an interface group, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Interface Groups**.

Step 4 From the Select a command drop-down list, choose **Add Interface Group**.

Step 5 Enter the necessary parameters:

- Name—User-defined name for this interface group (group1, group2).
- Interface Group Type—Select/deselect to quarantine a VLAN.
- Description—(Optional) Description for the Interface group.

Step 6 Click **Add**.

The Interface dialog box appears.

Step 7 Select the interfaces that you want to add to the group, and click **OK**.

To remove an Interface from the Interface group, from the Interface Group page, select the Interface and click **Remove**.

Step 8 Once you are done with adding the interfaces in the Interface Group page, click any of the following buttons:

- **Save** to confirm any changes made.
- **Audit** to audit the device values.
- **Cancel** to discard the changes.

Note

- The number of interfaces that can be added to an interface group depends upon the type of the controller.
- Guest LAN interfaces cannot be part of interface groups.
- An Interface group name must be different from the Interface name.

Deleting an Interface Group

To delete an interface group, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Interface Groups**.

Step 4 Select the check box of the interface group that you want to delete.

Step 5 From the Select a command drop-down list, choose **Delete Interface Group**, and click **Go**.

Step 6 Click **OK** to confirm the deletion.

Note

- The Interface Group cannot be deleted if it has been assigned to WLAN(s).
- The Interface Group cannot be deleted if it has been assigned to AP Group(s).

- The Interface Group cannot be deleted if it has been assigned to Foreign Controller Mapping for the WLAN(s).
- The Interface Group Template cannot be deleted if it has been assigned to WLAN Template(s).
- The Interface Group Template cannot be deleted if it has been assigned to AP Group Template(s).
- You cannot enable/disable quarantine for an interface if it has been assigned to an interface group.

Viewing Interface Groups

To view existing interface groups, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Interface Groups**. The following parameters appear:

- Name—User-defined name for the interface group (For example, group1, group2).
- Description—(Optional) Description for the Interface Group.
- Interfaces—Count of the number of interfaces belonging to the group.

Step 4 Click the Interface group name link.

The Interface Groups Details page appears with the Interface group details as well as the details of the Interfaces that form part of that particular Interface group.

NAC Integration

The Cisco NAC appliance, also known as Cisco Clean Access (CCA), is a Network Admission Control (NAC) product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether machines are compliant with security policies and repairs vulnerabilities before permitting access to the network. The NAC appliance is available in two modes: in-band and out-of-band. Customers can deploy both modes if desired, each geared toward certain types of access (in-band for supporting wireless users and out-of-band for supporting wired users, for example).

For more information on NAC Out-of-Band Integration, see the applicable section in the *Cisco Prime Network Control System Configuration Guide*.

This section contains the following topics:

- Guidelines for Using SNMP NAC, page 8-44
- Configuring NAC Out-of-Band Integration (SNMP NAC), page 8-45

Guidelines for Using SNMP NAC

Follow these guidelines when using SNMP NAC out-of-band integration:

- The NAC appliance supports up to 3500 users, and the controller supports up to 5000 users. Therefore, multiple NAC appliances might need to be deployed.

- Because the NAC appliance supports static VLAN mapping, you must configure a unique quarantine VLAN for each interface configured on the controller. For example, you might configure a quarantine VLAN of 110 on controller 1 and a quarantine VLAN of 120 on controller 2. However, if two WLANs or guest LANs use the same distribution system interface, they must use the same quarantine VLAN, provided they have one NAC appliance deployed in the network. The NAC appliance supports unique quarantine-to-access VLAN mapping.
- For posture reassessment based on session expiry, you must configure the session timeout on both the NAC appliance and the WLAN, making sure that the session expiry on the WLAN is greater than that on the NAC appliance.
- When a session timeout is configured on an open WLAN, the timing out of clients in the Quarantine state is determined by the timer on the NAC appliance. Once the session timeout expires for WLANs using web authentication, clients deauthenticate from the controller and must perform posture validation again.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching.
- If you want to enable NAC on an access point group VLAN, you must first enable NAC on the WLAN. Then you can enable or disable NAC on the access point group VLAN. If you ever decide to disable NAC on the WLAN, be sure to disable it on the access point group VLAN as well.
- NAC out-of-band integration is not supported for use with the WLAN AAA override feature.
- All Layer 2 and Layer 3 authentication occurs in the quarantine VLAN. To use external web authentication, you must configure the NAC appliance to allow HTTP traffic to and from external web servers and to allow the redirect URL in the quarantine VLAN.

Note See the Cisco NAC appliance configuration guides for configuration instructions at the following URL: http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html.

Guidelines for Using RADIUS NAC

Follow these guidelines when using RADIUS NAC:

- RADIUS NAC is available only for WLAN with 802.1x/WPA/WPA2 Layer 2 security.
- RADIUS NAC cannot be enabled when FlexConnect local switching is enabled.
- AAA override should be enabled to configure RADIUS NAC.

Configuring NAC Out-of-Band Integration (SNMP NAC)

To configure SNMP NAC out-of-band integration, follow these steps:

Step 1 To configure the quarantine VLAN for a dynamic interface, follow these steps:

a. Choose **Configure > Controller**.

b. Choose which controller you are configuring for out-of-band integration by clicking it in the IP Address column.

c. Choose **System > Interfaces** from the left sidebar menu.

d. Choose **Add Interface** from the Select a command drop-down list.

e. In the Interface Name text box, enter a name for this interface, such as “quarantine.”

f. In the VLAN Identifier text box, enter a non-zero value for the access VLAN ID, such as “10.”

g. Select the **Quarantine** check box if the interface has a quarantine VLAN ID configured on it.

Note We recommend that you configure unique quarantine VLANs throughout your network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in the same subnet, it is mandatory to have the same quarantine VLAN if there is only one NAC appliance in the network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in different subnets, it is mandatory to have different quarantine VLANs if there is only one NAC appliance in the network.

h. Configure any remaining fields for this interface, such as the IP address, netmask, and default gateway.

i. Enter an IP address for the primary and secondary DHCP server.

j. Click **Save**. You are now ready to create a NAC-enabled WLAN or Guest LAN.

Step 2 To configure NAC out-of-band support on a WLAN or guest LAN, follow these steps:

a. Choose **WLANs > WLAN** from the left sidebar menu.

b. Choose **Add a WLAN** from the Select a command drop-down list, and click **Go**.

c. If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the **click here** link to create a new template. For more information on setting up the template, see the “Configuring Wired Guest Access” section on page 8-47 section.

d. Click the **Advanced** tab.

e. To configure SNMP NAC support for this WLAN or guest LAN, choose **SNMP NAC** from the NAC Stage drop-down list. To disable SNMP NAC support, choose **None** from the NAC Stage drop-down list, which is the default value.

f. Click **Apply** to commit your changes.

Step 3 To configure NAC out-of-band support for a specific AP group, follow these steps:

a. Choose **WLANs > AP Groups VLAN** from the left sidebar menu to open the AP Groups page.

Note AP Groups (for 5.2 and later controllers) is referred to as AP Group VLANs for controllers prior to 5.2.

b. Click the name of the desired AP group.

c. From the Interface Name drop-down list, choose the quarantine enabled interface.

d. To configure SNMP NAC support for this AP group, choose **SNMP NAC** from the Nac State drop-down list. To disable NAC out-of-band support, choose **None** from the Nac State drop-down list, which is the default value.

e. Click **Apply** to commit your changes.

Step 4 To see the current state of the client (either Quarantine or Access), follow these steps:

a. Choose **Monitor > Clients** to open the Clients. Perform a search for clients.

b. Click the MAC address of the desired client to open the Clients > Detail page. The NAC state appears as access, invalid, or quarantine in the Security Information section.

Configuring Wired Guest Access

Wired Guest Access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room.

Like wireless guest user accounts, wired guest access ports are added to the network using the Lobby Ambassador feature. See the "Configuring Guest Account Settings" section on page 15-61.

Wired Guest Access can be configured in a standalone configuration or in a dual controller configuration employing an anchor and foreign controller. This latter configuration is used to further isolate wired guest access traffic but is not required for deployment of wired guest access.

Wired Guest Access ports initially terminate on a Layer 2 access switch or switch port which is configured with VLAN interfaces for wired guest access traffic.

The wired guest traffic is then trunked from the access switch to a wireless LAN controller. This controller is configured with an interface that is mapped to a wired guest access VLAN on the access switch.

If two controllers are being used, the controller (foreign) that receives the wired guest traffic from the switch then forwards the wired guest traffic to an anchor controller that is also configured for wired guest access. After successful hand off of the wired guest traffic to the anchor controller, a bidirectional Ethernet over IP (EoIP) tunnel is established between the foreign and anchor controllers to handle this traffic.

Note Although wired guest access is managed by anchor and foreign anchors when two controllers are deployed, mobility is not supported for wired guest access clients. In this case, DHCP and web authentication for the client are handled by the anchor controller.

Note You can specify how much bandwidth a wired guest user is allocated in the network by configuring and assigning a role and bandwidth contract. For details on configuring these features, see the "Configuring Guest Account Settings" section on page 15-61.

To configure and enable wired guest user access on the network, follow these steps:

Step 1 To configure a dynamic interface for wired guest user access, choose **Configure > Controllers** and after IP address, choose **System > Interfaces**.

Step 2 Choose **Add Interface** from the Select a command drop-down list, and click **Go**.

Step 3 Enter a name and VLAN ID for the new interface.

Step 4 Select the **Guest LAN** check box.

Step 5 Enter the primary and secondary port number.

Step 6 Click **Save**. You are now ready to create a wired LAN for guest access.

Step 7 To configure a wired LAN for guest user access, choose **WLANs > WLAN configuration** from the left sidebar menu.

Step 8 Choose **Add a WLAN** from the Select a command drop-down list, and click **Go**.

Step 9 If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the **click here** link to create a new template.

Step 10 In the WLAN > New Template general page, enter a name in the Profile Name text box that identifies the guest LAN. Do not use any spaces in the name entered.

Step 11 Select the **Enabled** check box for the WLAN Status field.

Step 12 From the Ingress Interface drop-down list, choose the VLAN that you created in Step 3. This VLAN provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 13 From the Egress Interface drop-down list, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic.

Note If you have only one controller in the configuration, choose **management** from the Egress Interface drop-down list.

Step 14 Click the **Security > Layer 3** tab to modify the default security policy (web authentication) or to assign WLAN specific web authentication (login, logout, login failure) pages and the server source.

a. To change the security policy to passthrough, select the **Web Policy** check box and select the **Passthrough** radio button. This option allows users to access the network without entering a username or password.

An Email Input check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

b. To specify custom web authentication pages, unselect the Global WebAuth Configuration **Enabled** check box.

When the Web Auth Type drop-down list appears, choose one of the following options to define the web login page for the wireless guest users:

Default Internal—Displays the default web login page for the controller. This is the default value.

Customized Web Auth—Displays custom web login, login failure, and logout pages. When the customized option is selected, three separate drop-down lists for login, login failure, and logout page selection appear. You do not need to define a customized page for all three of the options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option.

These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files. For specifics on downloading custom pages, see the "Downloading a Customized WebAuthentication Bundle to a Controller" section on page 8-16.

External—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

You can select specific RADIUS or LDAP servers to provide external authentication in the Security > AAA pane. To do so, continue with Step 17.

Note The RADIUS and LDAP external servers must be already configured to have selectable options in the Security > AAA pane. You can configure these servers on the RADIUS Authentication Servers, TACACS+ Authentication Servers page, and LDAP Servers page.

Step 15 If you selected External as the Web Authentication Type in Step 15, choose **Security > AAA** and choose up to three RADIUS and LDAP servers using the drop-down lists.

Step 16 Click **Save**.

Step 17 Repeat this process if a second (anchor) controller is being used in the network.

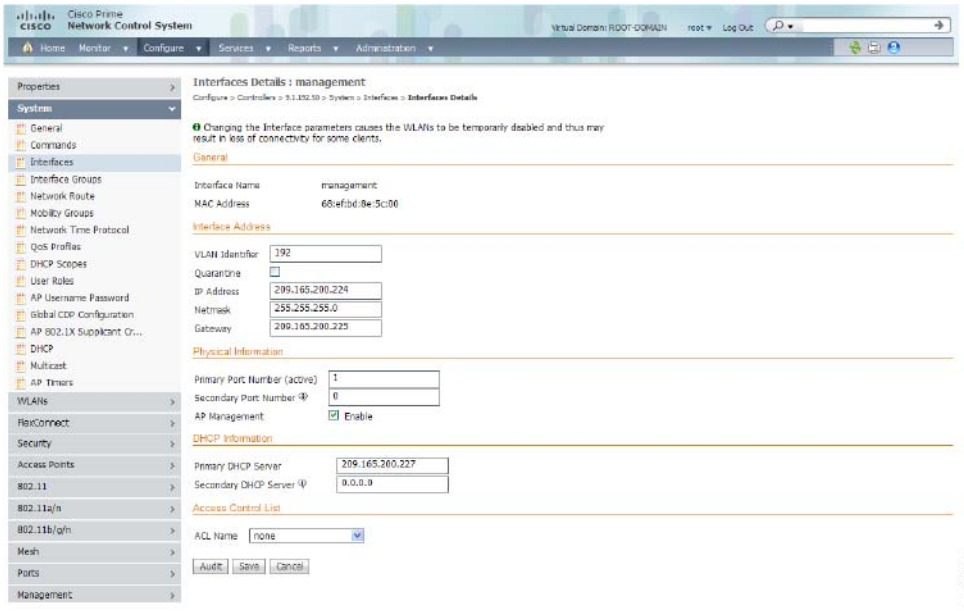
Creating an Ingress Interface

To create an Ingress interface, follow these steps:

Step 1 Choose **Add Interface** from the Select a command drop-down list, and click **Go**.

Step 2 Click an interface name. The Interfaces Details : New Config page appears (see Figure 8-3).

Figure 8-3 Interfaces Details : New Config Page



Step 3 In the Interface Name text box, enter a name for this interface, such as guestinterface.

Step 4 Enter a VLAN identifier for the new interface.

Step 5 Select the **Guest LAN** check box.

Step 6 Enter the primary and secondary port numbers.

Step 7 Click **Save**.

Creating an Egress Interface

To create an Egress interface, follow these steps:

Step 1 Choose **Add Interface** from the Select a command drop-down list, and click **Go**.

Step 2 Click an interface name. The Interfaces Details : New Config page appears (see Figure 8-3).

Step 3 In the Interface Name text box, enter a name for this interface, such as quarantine.

Step 4 In the VLAN Identifier text box, enter a non-zero value for the access VLAN ID, such as 10.

Step 5 Select the **Quarantine** check box and enter a non-zero value for the quarantine VLAN ID, such as 110.

Note You can have NAC-support enabled on the WLAN or guest WLAN template Advanced tab for interfaces with Quarantine enabled.

Step 6 Enter the IP address, netmask, and default gateway.

Step 7 Enter the primary and secondary port numbers.

Step 8 Provide an IP address for the primary and secondary DHCP server.

Step 9 Configure any remaining fields for this interface, and click **Save**.

You are now ready to create a wired LAN for guest access.

Configuring Controller Network Routes

The Network Route page enables you to add a route to the controller service port. This route allows you to direct all Service Port traffic to the designated management IP address.

- Viewing Existing Network Routes, page 8-50
- Adding a Network Route, page 8-50

Viewing Existing Network Routes

To view existing network routes, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Network Route**. The following parameters appear:

- IP Address—The IP address of the network route.
- IP Netmask—Network mask of the route.
- Gateway IP Address—Gateway IP address of the network route.

Adding a Network Route

To add a network route, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Network Route**.

Step 4 From the Select a command drop-down list, choose **Add Network Route**.

Step 5 Click **Go**.

Step 6 Enter the IP address, IP Netmask, and Gateway IP address information.

Step 7 Click **Save**.

Configuring Controller Spanning Tree Protocol Parameters

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

To view or manage current STP parameters, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Spanning Tree Protocol**. The Spanning Tree Protocol page displays the following parameters:

- Protocol Spec—The current protocol specification.
- Admin Status—Select this check box to enable.
- Priority—The numerical priority number of the ideal switch.
- Maximum Age (seconds)—The amount of time (in seconds) before the received protocol information recorded for a port is discarded.
- Hello Time (seconds)—Determines how often (in seconds) the switch broadcasts its hello message to other switches.
- Forward Delay (seconds)—The time spent (in seconds) by a port in the learning/listening states of the switches.

Configuring Controller Mobility Groups

By creating a mobility group, you can enable multiple network controllers to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers can share the context and state of client devices and controller loading information. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.

Note If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be in the same mobility group.

- Messaging Among Mobility Groups, page 8-52
- Mobility Group Prerequisites, page 8-52
- Viewing Current Mobility Group Members, page 8-52
- Adding Mobility Group Members from a List of Controllers, page 8-52
- Manually Adding Mobility Group Members, page 8-53
- Setting the Mobility Scalability Parameters, page 8-53

Messaging Among Mobility Groups

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers:

- There can be up to 72 members in the list with up to 24 in the same mobility group.
- The controller sends a Mobile Announce message to members in the mobility list each time a new client associates to it.
- In the NCS and controller software release 5.0, the controller uses multicast mode to send the Mobile Announce messages. This allows the controller to send only one copy of the message to the network, which delivers it to the multicast group containing all the mobility members.

Note For more information regarding mobility groups, see the *Cisco Prime Network Control System Configuration Guide*.

Mobility Group Prerequisites

Before you add controllers to a mobility group, you must verify that the following requirements have been met for all controllers that are to be included in the group:

- All controllers must be configured for the same CAPWAP transport mode (Layer 2 or Layer 3).
- IP connectivity must exist between the management interfaces of all devices.
- All controllers must be configured with the same mobility group name.
- All devices must be configured with the same virtual interface IP address.
- Availability of MAC and IP addresses of each controller to be included in the mobility group (to configure the controllers with the MAC address and IP address of all the other mobility group members).

Viewing Current Mobility Group Members

To view current mobility group members, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Mobility Groups**.

Note To delete a group member, select a check box for the applicable group member, choose **Delete Group Members**, and click **Go**.

Adding Mobility Group Members from a List of Controllers

To add a mobility group member from a list of existing controllers, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Mobility Groups**.

Step 4 From the Select a command drop-down list, choose **Add Group Members**.

Step 5 Click **Go**.

Step 6 Select the check box(es) for the controller to be added to the mobility group.

Step 7 Click **Save**.

Manually Adding Mobility Group Members

If no controllers were found to add to the mobility group, you can add members manually. To manually add members to the mobility group, follow these steps:

Step 1 Click the **click here** link from the Mobility Group Member details page.

Step 2 In the Member MAC Address text box, enter the MAC address of the controller to be added.

Step 3 In the Member IP Address text box, enter the management interface IP address of the controller to be added.

Note If you are configuring the mobility group in a network where Network Address Translation (NAT) is enabled, enter the IP address sent to the controller from the NAT device rather than the controller management interface IP address. Otherwise, mobility fails among controllers in the mobility group.

Step 4 Enter the multicast group IP address to be used for multicast mobility messages in the Multicast Address text box. The local mobility member group address must be the same as the local controller group address.

Step 5 In the Group Name text box, enter the name of the mobility group.

Step 6 Click **Save**.

Step 7 Repeat Steps 1 through 6 for the remaining WLC devices.

Setting the Mobility Scalability Parameters

Note Mobility Groups must be configured prior to setting the mobility scalability parameters.

To set the mobility message parameters, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address of a controller whose software version is 5.0 or later.

Step 3 From the left sidebar menu, choose **System > General**.

Step 4 From the Multicast Mobility Mode drop-down list, specify if you want to enable or disable the ability for the controller to use multicast mode to send Mobile Announce messages to mobility members.

Step 5 If you enabled multicast messaging by setting multicast mobility mode to enabled, you must enter the group IP address at the Mobility Group Multicast-address field to begin multicast mobility messaging. You must configure this IP address for the local mobility group but it is optional for other groups within the mobility list. If you do not configure the IP address for other (non-local) groups, the controllers use unicast mode to send mobility messages to those members.

Step 6 Click **Save**.

Configuring Controller Network Time Protocol

To add a new NTP Server, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Network Time Protocol**.

Step 4 From the Select a command drop-down list, choose **Add NTP Server**.

Step 5 Click **Go**.

Step 6 From the Select a template to apply to this controller drop-down list, choose the applicable template to apply to this controller.

Command Buttons

- Apply
- Cancel

To create a New Template for NTP Servers, use the **click here** link to access the template creation page (Configure NTP Servers > New Template).

NTP general parameters include the following:

- Template Name—Enter the new NTP Template name.

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Server Address—Enter the NTP server IP address.
- No. of Controllers Applied To—Number of controllers to which this template is applied (read-only).

Background Scanning on 1510s in Mesh Networks

Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents. Because the access points are searching on neighboring channels as well as the current channel, the list of optimal alternate paths and parents is greater.

Identifying this information prior to the loss of a parent results in a faster transfer and the best link possible for the access points. Additionally, access points might switch to a new channel if a link on that channel is found to be better than the current channel in terms of fewer hops, stronger signal-to-noise ratio (SNR), and so on.

Background scanning on other channels and data collection from neighbors on those channels are performed on the primary backhaul between two access points:

The primary backhaul for 1510s operate on the 802.11a link.

Background scanning is enabled on a global basis on the associated controller of the access point.

Note Latency might increase for voice calls when they are switched to a new channel.

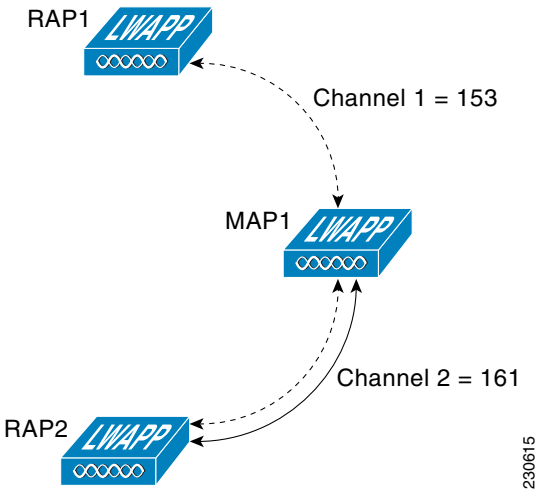
Note In the EMEA regulatory domain, locating neighbors on other channels might take longer given DFS requirements.

Background Scanning Scenarios

A few scenarios are provided below to better illustrate how background scanning operates.

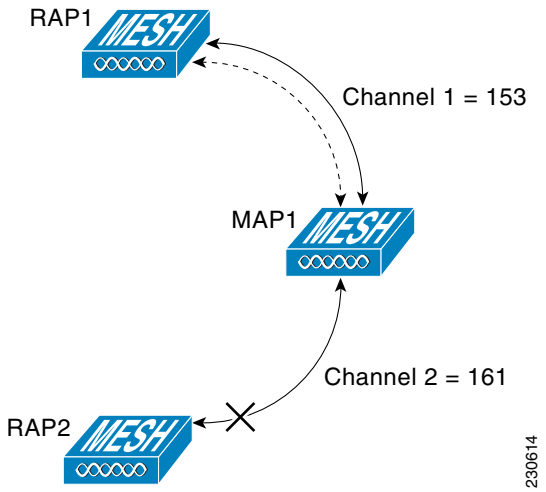
In Figure 8-4, when the mesh access point (MAP1) initially comes up, it is aware of both root access points (RAP1 and RAP2) as possible parents. It chooses RAP2 as its parent because the route through RAP2 is better in terms of hops, SNR, and so on. After the link is established, background scanning (once enabled) continuously monitors all channels in search of a more optimal path and parent. RAP2 continues to act as parent for MAP1 and communicates on channel 2 until either the link goes down or a more optimal path is located on another channel.

Figure 8-4 Mesh Access Point (MAP1) Selects a Parent



In Figure 8-5, the link between MAP1 and RAP2 is lost. Data from ongoing background scanning identifies RAP1 and channel 1 as the next best parent and communication path for MAP1 so that link is established immediately without the need for additional scanning after the link to RAP2 goes down.

Figure 8-5 Background Scanning Identifies a New Parent



Enabling Background Scanning

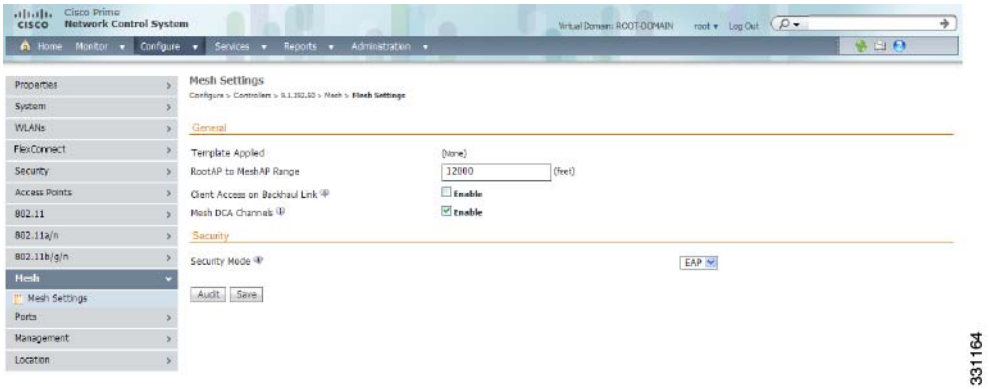
To enable background scanning on an AP1510 RAP or MAP, follow these steps:

Step 1 Choose **Configure > Controllers**.

Note You can also enable this on the Controllers template. See the "Configuring Mesh Templates" section on page 10-122.

Step 2 Choose **Mesh > Mesh Settings** from the left sidebar menu. The Mesh Settings page appears (see Figure 8-6).

Figure 8-6 Mesh Settings Page



Step 3 Select the **Background Scanning** check box to enable background scanning or unselect it to disable the feature. The default value is disabled.

Step 4 Click **Save**.

Configuring Controller QoS Profiles

To make modifications to the quality of service profiles, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > QoS Profiles**. The following parameters appear:

- Bronze—For Background
- Gold—For Video Applications
- Platinum—For Voice Applications
- Silver—For Best Effort

Step 4 Click the applicable profile to view or edit profile parameters.

Step 5 Set the following values in the Per-User Bandwidth Contracts group box (all have a default of 0 or Off):

- Average Data Rate—The average data rate for non-UDP traffic.
- Burst Data Rate—The peak data rate for non-UDP traffic.
- Average Real-time Rate—The average data rate for UDP traffic.
- Burst Real-time Rate—The peak data rate for UDP traffic.

Step 6 Set the following values for the Over-the-Air QoS group box:

- Maximum QoS RF Usage Per AP (%)—The maximum air bandwidth available to clients. The default is 100%.
- QoS Queue Depth—The depth of queue for a class of client. The packets with a greater value are dropped at the access point.

Step 7 Set the following values in the WLAN QoS group box:

- Maximum Priority
- Unicast Default Priority
- Multicast Default Priority

Step 8 Set the following value in the Wired QoS Protocol group box:

- Wired QoS Protocol—Choose **802.1P** to activate 802.1P priority tags or **None** to deactivate 802.1P priority tags.

Step 9 Click **Save**.

Configuring Controller DHCP Scopes

This section contains the following topics:

Viewing Current DHCP Scopes

To view current DHCP (Dynamic Host Configuration Protocol) scopes, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > DHCP Scopes**.

The following DHCP Scopes information appears:

- Pool Address
- Lease Time
- Status

Adding a New DHCP Scope

To add a new DHCP Scope, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > DHCP Scopes**.

Step 4 From the Select a command drop-down list, choose **Add DHCP Scope**.

Step 5 Enter the following information:

- Scope Name
- Lease Time (in seconds)
- Network
- Netmask
- Pool Start Address
- Pool End Address
- DNS Domain Name
- Status
- Router Addresses—Enter which IP addresses are already in use and should therefore be excluded. For example, you should enter the IP address of your company router. In doing so, this IP address is blocked from use by another client.
- DNS Servers—Enter the IP address of the DNS server(s). Each DNS server must be able to update a client DNS entry to match the IP address assigned by this DHCP scope.
- NetBios Servers—Enter the IP address of the Microsoft Network Basic Input Output System (NetBIOS) name server(s), such as a Windows Internet Naming Service (WINS) server.

Step 6 Click **Save**.

Configuring Controller User Roles

This section contains the following topics:

- Adding a New Local Net User Role, page 8-59

Viewing Current Local Net User Roles

To view current local net user roles, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > User Roles**.

The following Local Net User Role parameters appear:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Role Name
- Average Data Rate—The average data rate for non-UDP traffic.
- Burst Data Rate—The peak data rate for non-UDP traffic.
- Average Real-time Rate—The average data rate for UDP traffic.
- Burst Real-time Rate—The peak data rate for UDP traffic.

Step 4 Click a Template Name to view the User Role details.

Adding a New Local Net User Role

To add a new local net user role, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > User Roles**.

Step 4 From the Select a command drop-down list, choose **Add User Role**.

Step 5 Select a template from the Select a template to apply to this controller drop-down list.

Step 6 Click **Apply**.

Note To create a new template for local net user roles, click the **click here** link to access the template creation page. See the "Configuring User Roles Controller Templates" section on page 10-11 for more information about User Role templates.

Configuring a Global Access Point Password

The AP Username Password page enables you to set a global password that all access points inherit as they join a controller. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis. See the "Configuring AP Configuration Templates" section on page 10-137 to view where the global password is displayed and how it can be overridden on a per-access point basis.

Also in controller software release 5.0, after an access point joins the controller, the access point enables console port security and you are prompted for your username and password whenever you log into the access point console port. When you log in, you are in non-privileged mode and you must enter the enable password to use the privileged mode.

To establish a global username and password, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address of a controller with a Release 5.0 or later.

Step 3 From the left sidebar menu, choose **System > AP Username Password**.

Step 4 Enter the username and password that you want to be inherited by all access points that join the controller.

Note For Cisco IOS access points, you must also enter and confirm an enable password.

Step 5 Click **Save**.

Configuring Global CDP

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

Note CDP is enabled on the Ethernet and radio ports of a bridge by default.

Note Global Interface CDP configuration is applied to only the APs with CDP enabled at AP level.

To configure a Global CDP, perform the following steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the IP address of the desired controller.

Step 3 From the left sidebar menu, choose **System > Global CDP Configuration** from the left sidebar menu. The Global CDP Configuration page appears.

Step 4 In the Global CDP group box, configure the following parameters:

- CDP on controller—Choose enable or disable CDP on the controller.

Note This configuration cannot be applied on WiSM2 controllers.

- Global CDP on APs—Choose to enable or disable CDP on the access points.
- Refresh-time Interval (seconds)—In the Refresh Time Interval field, enter the time in seconds at which CDP messages are generated. The default is 60.
- Holdtime (seconds)—Enter the time in seconds before the CDP neighbor entry expires. The default is 180.
- CDP Advertisement Version—Enter which version of the CDP protocol to use. The default is v1.

Step 5 In the CDP for Ethernet Interfaces group box, select the slots of Ethernet interfaces for which you want to enable CDP.

Note CDP for Ethernet Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 6 In the CDP for Radio Interfaces group box, select the slots of Radio interfaces for which you want to enable CDP.

Note CDP for Radio Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 7 Click **Save**.

Configuring AP 802.1X Supplicant Credentials

You can configure 802.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning. You can set global authentication settings that all access points inherit as they join the controller. This includes all access points that are currently joined to the controller and any that join in the future.

If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point. See the "Configuring Access Point Details" section on page 8-174 for more information.

To enable global supplicant credentials, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the IP address of the desired controller.

Step 3 From the left sidebar menu, choose **System > AP 802.1X Supplicant Credentials**.

Step 4 Select the **Global Supplicant Credentials** check box.

Step 5 Enter the supplicant username.

Step 6 Enter and confirm the applicable password.

Step 7 Click **Save**.

Note Once saved, you can click **Audit** to perform an audit on this controller. See the "Understanding the Controller Audit Report" section on page 8-3 or the "Configuring an Audit" section on page 15-53 for more information.

Configuring Controller DHCP

To configure DHCP (Dynamic Host Configuration Protocol) information for a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the IP address of the desired controller.

Step 3 From the left sidebar menu, choose **System > DHCP**.

Step 4 Add or modify the following parameters:

- DHCP Option 82 Remote Id Field Format—Choose **AP-MAC** or **AP-MAC-SSID** from the drop-down list.

  Note To set the format for RemoteID field in DHCP option 82
  If Ap-Mac is selected, then set the RemoteID format as *AP-Mac*. If Ap-Mac-ssid is selected, then set the RemoteID format as *AP-Mac:SSID*.

- DHCP Proxy—Select the check box to enable DHCP by proxy.

  Note When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the WLAN or the WLAN itself.

Step 5 Enter the DHCP Timeout in seconds after which the DHCP request times out. The default setting is 5. Allowed values range from 5 to 120 seconds.

Note DHCP Timeout is applicable for Controller Release 7.0.114.74 and later.

Step 6 Click **Save**.

Note Once saved, you can click **Audit** to perform an audit on this controller. See the "Understanding the Controller Audit Report" section on page 8-3 or the "Configuring an Audit" section on page 15-53 for more information.

Configuring Controller Multicast Mode

The NCS provides an option to configure IGMP (Internet Group Management Protocol) snooping and timeout values on the controller.

To configure multicast mode and IGMP snooping for a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the desired controller.

Step 3 From the left sidebar menu, choose **System > Multicast**.

Step 4 Choose **Disable**, **Unicast**, or **Multicast** from the Ethernet Multicast Support drop-down list.

Note IGMP Snooping and timeout can be set only if Ethernet Multicast mode is Enabled.

Step 5 If Multicast is selected, enter the multicast group IP address.

Step 6 Select the Enable Global Multicast Mode check box to make the multicast mode available globally.

Step 7 Select to enable IGMP Snooping.

Step 8 Choose **Enable** from the Multicast Mobility Mode drop-down list to change the IGMP snooping status or to set the IGMP timeout. When IGMP snooping is enabled, the controller gathers IGMP reports from the clients and then sends each access point a list of the clients listening to any multicast group. The access point then forwards the multicast packets only to those clients.

The timeout interval has a range of 3 to 300 and a default value of 60. When the timeout expires, the controller sends a query to all WLANs. Those clients which are listening in the multicast group then send a packet back to the controller.

Step 9 If you enabled the Multicast Mobility Mode, enter the mobility group multicast address.

Step 10 Select the **Multicast Direct feature** check box to enable videos to be streamed over a wireless network.

Step 11 Choose **Enable** from the Multicast Mobility Mode drop-down list to change MLD configuration.

Step 12 Select the **Enable MLD Snooping** check box to enable IPv6 MLD snooping. If you have selected this check box, configure the following parameters:

- MLD Timeout—Enter the MLD timeout value in seconds. The timeout has a range of 3 to 7200 and a default value of 60.
- MLD Query Interval—Enter the MLD query interval timeout value in seconds. The interval has a range of 15 to 2400 and a default value of 20.

Note Internet Group Management Protocol (IGMP) snooping enables you to limit the flooding of multicast traffic for IPv4. For IPv6, Multicast Listener Discovery (MLD) snooping is used.

Step 13 Specify the Session Banner information, which is the error information sent to the client if the client is denied or dropped from a Media Stream.

a. State—Select the check box to activate the Session Banner. If not activated, the Session Banner is not sent to the client.

b. URL—A web address reported to the client

c. Email—An e-mail address reported to the client

d. Phone—A telephone number reported to the client

e. Note—A note reported to the client

Note All Media Streams on a Controller share this configuration.

Step 14 Click **Save**.

Note Once saved, you can click **Audit** to perform an audit on this controller. See the "Understanding the Controller Audit Report" section on page 8-3 or the "Configuring an Audit" section on page 15-53 for more information.

Configuring Access Point Timer Settings

Advanced timer configuration for FlexConnect and local mode is available for the controller on the NCS.

Note This feature is only supported on Release 6.0 controllers and later.

Configuring Advanced Timers

To configure the advanced timers, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the controller for which you want to set timer configuration.

Step 3 From the left sidebar menu, choose **System > AP Timers**.

Step 4 Select the applicable access point mode (Local mode or FlexConnect mode).

Step 5 See the "Access Point Timer Settings for Local Mode" section on page 8-64 or the "Access Point Timer Settings for FlexConnect Mode" section on page 8-64 for more information on each mode configuration.

Access Point Timer Settings for Local Mode

To reduce the failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller. You can then enter a value between 10 and 15 seconds.

Access Point Timer Settings for FlexConnect Mode

Once selected, you can configure the FlexConnect timeout value. Select the **AP Primary Discovery Timeout** check box to enable the timeout value. Enter a value between 30 and 3600 seconds.

Note 5500 series controllers accept access point fast heartbeat timer values in the range of 1-10.

Configuring Controller WLANs

Because controllers can support 512 WLAN configurations, the NCS provides an effective way to enable or disable multiple WLANs at a specified time for a given controller.

To view a summary of the wireless local access networks (WLANs) that you have configured on your network, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **WLANs > WLAN Configuration**. The Configure WLAN Summary page appears (see Figure 8-7). This WLAN Configuration page contains the values found in Table 8-1.

Figure 8-7 WLAN Configuration Summary Page

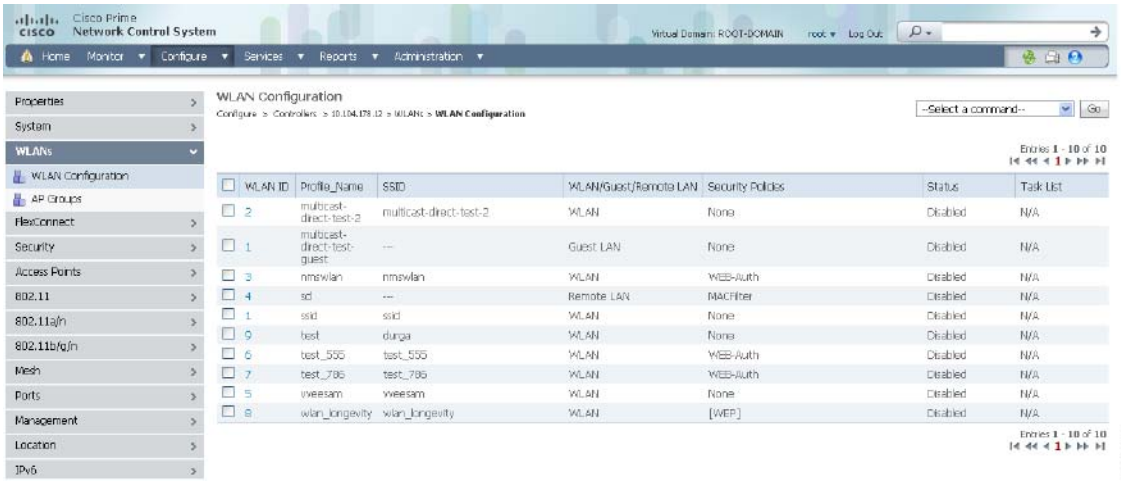


Table 8-1 WLAN Configuration Summary Page

Field	Description
Check box	Select the WLAN for deletion. Choose **Delete WLANs** from the Select a command drop-down list.
WLAN ID	Identification number of the WLAN.
Profile Name	User-defined profile name specified when creating the WLAN template. Profile Name is the WLAN name.
SSID	Service Set Identifier being broadcast by.

Table 8-1 WLAN Configuration Summary Page (continued)

Field	Description
WLAN/Guest LAN	Specifies if it is a WLAN or guest LAN.
Security Policies	Security policies enabled on the WLAN.
Status	Status of the WLAN is either enabled or disabled.
Task List	If a task is scheduled in Configure > Scheduled Configuration Tasks, you have a link to view the scheduled configuration task.

Viewing WLAN Details

To view WLAN details, choose **WLANs**. The WLAN Details page appears.

Use the tabs (General, Security, QoS, and Advanced) to view or edit parameters for the WLAN.

This section contains the following topics:

General Tab

The General tab includes the following information:

Note Depending on the WLAN template used for this controller, these parameters might or might not be available.

- Guest LAN—Indicates whether or not this WLAN is a Guest LAN.
- Profile Name
- SSID
- Status—Select the Enabled check box to enable this WLAN.

  Note To configure a start time for the WLAN status to be enabled, select the **Schedule Status** check box. Choose the hours and minutes from the drop-down lists. Click the calendar icon to select the applicable date.

- Schedule Status
- Security Policies—Identifies the security policies set using the Security tab (includes security policies such as None, 802.1X, Static WEP, Static WEP-802.1X, WPA+WPA2, and CKIP). Changes to the security policies appear after the page is saved.
- Radio Policy—Choose any of the following from the drop-down list:

  - **All**, **802.11a only**, **802.11g only**, **802.11b/g only**, **802.11a/g only**.
- Interface/Interface Group—Choose from the drop-down list.
- Broadcast SSID—Select the check box to enable.
- Egress Interface—Select the name of the applicable interface. This WLAN provides a path out of the controller for wired guest client traffic.

Note If you only have one controller in the configuration, choose **Management** from the Egress Interface drop-down list.

- Ingress Interface—Choose the applicable VLAN from the drop-down list. This interface provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Security Tab

The Security tab includes three additional tabs: Layer 2, Layer 3, and AAA Servers.

Layer 2 Security

Use the Layer 2 Security drop-down list to choose between **None**, **802.1x**, **Static WEP**, **Cranite**, **Static WEP-802.1x**, **WPA1+WPA2**, and **CKIP**. These parameters are described in the Table 8-2.

Mac Filtering—Select the check box if you want to filter clients by MAC address.

Note Mac Filtering, Max-Clients, Client Profiling are not supported with FlexConnect Local Authentication.

Table 8-2 Layer 2 Security Options

Field	Description
None	• No Layer 2 security selected. – FT Enable—Select the check box to enable Fast Transition (FT) between access points. **Note** The fast transition feature is not supported with FlexConnect mode. – Over the DS—Select the check box to enable the fast transition over a distributed system. – Reassociation Timeout—Time in seconds after which fast transition reassociation times out. The default is 20 seconds, and the valid range is 1 to 100. **Note** To enable Over the DS or Reassociation Timeout, you should enable fast transition.
802.1x	802.11 Data Encryption: • Type—WEP • Key Size—40, 104, or 128 bits.

Table 8-2 Layer 2 Security Options (continued)

Field	Description
Static WEP	802.11 Data Encryption: • Type • Key Size—Not set, 40, 104, or 128 bits. • Key Index—1 to 4. • Encryption Key • Encryption Key Format—ASCII or HEX. • Allowed Shared Key Authentication—Select the check box to enable shared key authentication.
Cranite	Configure the WLAN to use the FIPS140-2 compliant Cranite Wireless Wall Software Suite, which uses AES encryption and VPN tunnels to encrypt and verify all data frames carried by the Cisco Wireless LAN Solution.
Static WEP-802.1X	Use this setting to enable both Static WEP and 802.1X policies. If this option is selected, static WEP and 802.1X parameters are displayed at the bottom of the page. Static WEP encryption parameters: • 802.11 Data Encryption – Type – Key Size—Not set, 40, 104, or 128 bits. – Key Index—1 to 4. – Encryption Key – Encryption Key Format—ASCII or HEX. • Allowed Shared Key Authentication—Select the check box to enable.

Table 8-2 Layer 2 Security Options (continued)

Field	Description
WPA+WPA2	Use this setting to enable WPA, WPA2, or both. WPA enables Wi-Fi Protected Access with TKIP-MIC Data Encryption or AES. When WPA+WPA2 is selected, you can use Cisco Centralized Key Management (CCKM) authentication key management, which allows fast exchange when a client roams from one access point to another. When WPA+WPA2 is selected as the Layer 2 security policy and preshared key is enabled, neither CCKM nor 802.1X can be enabled; although, both CCKM and 802.1X can be enabled at the same time. • Mac Filtering—Enables MAC address filtering. **Note** Mac Filtering and Max-Clients are not supported with FlexConnect Local Authentication. • FT Enable—Select the check box to enable fast transition between access points. **Note** Fast transition is not supported with FlexConnect mode. – Over the DS—Select the check box to enable the fast transition over a distributed system. – Reassociation Timeout—Time in seconds after which fast transition reassociation times out. The default is 20 seconds, and the valid range is 1 to 100. **Note** To enable Over the DS or Reassociation Timeout, fast transition should be enabled. WPA+WPA2 parameters: • WPA1—Select the check box to enable WPA1. • WPA2—Select the check box to enable WPA2. Authentication Key Management: • FT802.1X—Select the check box to enable FT802.1X. • 802.1X—Select the check box to enable 802.1X. • CCKM—Select the check box to enable CCKM. • PSK—Select the check box to enable PSK. • FTPSK—Select the check box to enable FTPSK. **Note** Enable WPA2 and fast transition to set FT802.1X or FTPSK.

Table 8-2 Layer 2 Security Options (continued)

Field	Description
CKIP	Cisco Key Integrity Protocol. A Cisco access point advertises support for CKIP in beacon and probe response packets. CKIP can be configured only when Aironet IE is enabled on the WAN. **Note** CKIP is not supported on 10xx access points. CKIP parameters: • 802.11 Data Encryption – Type – Key Size—Not set, 40, 104, or 128 bits. – Key Index—1 to 4. – Encryption Key – Encryption Key Format—ASCII or HEX. • MMH Mode—Select the check box to enable. • Key Permutation—Select the check box to enable.

Layer 3 Security

Use the Layer 3 Security drop-down list to choose between **None**, **VPN Pass Through**, and **IPsec (Internet Protocol Security)**. The page parameters change according to the selection you make.

Note Depending on the type of WLAN, the Layer 3 parameters might or might not be available.

Note If you choose VPN pass through, you must enter the VPN gateway address.

Note IPsec is a suite of protocols for securing IP communications by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for establishing cryptographic keys.

Web Policy—Select the check box to specify policies such as authentication, pass through, conditional web redirect, or WebAuth on MAC Filter Failure. This section also allows you to enable guest users to view customized login pages.

Note If you choose Pass Through, the Email Input check box appears. Select this check box if you want users to be prompted for their e-mail addresses when attempting to connect to the network.

Preauthentication ACL—Lists IPv4, IPv6, and WebAuth ACLs to be used for traffic between the client and the controller.

Note IPv6 ACL mapping for WLANs is supported from Controller Release 7.2.x.

To allow guest users to view customized login pages, follow these steps:

Step 1 Unselect the **Global WebAuth Configuration** check box.

Step 2 Choose **Web Auth Type** from the drop-down list on the Security > Layer 3 tab.

- Default Internal—The guest user receives the default login page.
- Customized WebAuth—Customized login pages can be downloaded from the Upload/Download Commands page. See the "Downloading a Customized Web Authentication Page" section on page 10-69 for more information.
  - Choose **Web Auth Login Page**, **Web Auth Login Failure Page**, or **Web Auth Logout Page** from the drop-down lists.
  - Choose **None** from any of the drop-down lists if you do not want to display a customized page for that option.
- External—The guest user is redirected to an external login page. Enter the login page URL in the External Web Auth URL text box.

Note If External is selected, you can select up to three RADIUS and LDAP servers in the Security > AAA page. See the "AAA Servers" section on page 8-71 for more information.

AAA Servers

Select RADIUS and LDAP servers to override use of default servers on the current WLAN.

- RADIUS Servers—Use the drop-down lists to choose authentication and accounting servers. With this selection, the default RADIUS server for the specified WLAN overrides the RADIUS server that is configured for the network. If all three RADIUS servers are configured for a particular WLAN, server 1 has the highest priority, and so on.
- LDAP Servers—If no LDAP servers are chosen from the drop-down lists, the NCS uses the default LDAP server order from the database.
- Local EAP Authorization—Allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the back-end system becomes disrupted or the external authentication server fails.

  Select the check box to enable if you have an EAP profile configured. Select the profile from the drop-down list.
- Allow AAA Override—When enabled, if a client has conflicting AAA and controller WLAN authentication parameters, client authentication is performed by the AAA server.

  As part of this authentication, the operating system moves clients from the default Cisco WLAN solution to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, or WPA operation).

  In all cases, the operating system also uses QoS and ACL provided by the AAA server as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as *identity networking*.)

When AAA override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is only performed by the AAA server if the controller WLANs do not contain any client-specific authentication parameters.

QoS Tab

- Quality of service (QoS)—From the drop-down list, choose **Platinum** (voice), **Gold** (video), **Silver** (best effort), or **Bronze** (background).
  - Services such as VoIP should be set to gold. Non-discriminating services such as text messaging can be set to bronze.
- WMM Parameters
  - WMM Policy—Choose **Disabled**, **Allowed** (to allow clients to communicate with the WLAN), or **Required** (to make it mandatory for clients to have WMM enabled for communication).
  - 7920 AP CAC—Select the check box to enable support on Cisco 7920 phones.
  - 7920 Client CAC—Select the check box to enable WLAN support for older versions of the software on 7920 phones. The CAC limit is set on the access point for newer versions of software.

Advanced Tab

- FlexConnect Local Switching—Select this check box to enable FlexConnect local switching. When enabled, the FlexConnect access point handles client authentication and switches client packets locally. See the "Configuring FlexConnect" section on page 12-4 for more information.

Note FlexConnect local switching applies only to Cisco 1130/1240/1250 series access points. It is not supported with L2TP, PPTP, CRANITE, and FORTRESS authentications. It does not apply to WLAN IDs 9-16.

- Enable FlexConnect local authentication by selecting the **FlexConnect Local Auth** check box.

  Local authentication is useful where you cannot maintain the criteria, which is a remote office setup of minimum bandwidth of 128 kbps with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local switching, the authentication capabilities are present in the access point itself. Therefore, local authentication reduces the latency requirements of the branch office.

Note Local authentication can only be enabled on the WLAN of a FlexConnect AP that is in local switching mode.

  Local authentication is not supported in the following scenarios:

  - Guest Authentication cannot be performed on a FlexConnect local authentication-enabled WLAN.
  - RRM information is not available at the controller for the FlexConnect local authentication-enabled WLAN.
  - Local RADIUS is not supported.
  - Once the client has been authenticated, roaming is supported only after the WLC and the other FlexConnects in the group are updated with the client information.

- Session Timeout (secs)—Set the maximum time a client session can continue before reauthentication.
- Override Interface ACL—Lists IPv4 and IPv6 access control list (ACL) that overrides the ACL configured for the interface on this WLAN.
- Learn Client IP Address—When you enable hybrid-REAP local switching, the Learn Client IP Address check box is enabled by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client IP address, and the controller periodically drops the client. Disable this option so that the controller maintains the client connection without waiting to learn the client IP address. The ability to disable this option is supported only with hybrid-REAP local switching; it is not supported with hybrid-REAP central switching.
- Aironet IE—Select the check box to enable support for Aironet information elements (IEs) for this WLAN.
  - If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the association request.
- IPv6—Select the check box to enable IPv6.

Note Layer 3 security must be set to None for IPv6 to be enabled.

- Diagnostic Channel—Click to enable the diagnostics. When enabled, clients can connect to this WLAN for diagnostic purposes.

Note The results of the diagnostic tests are stored in the SNMP table, and the NCS polls these tables to display the results.

- Override Interface ACL—Choose a defined access control list (ACL) from the drop-down list. When the ACL is selected, the WLAN associates the ACL to the WLAN.

Note Choosing an ACL is optional, and the default is None.

For more information, see the "Configuring an Access Control List Template" section on page 10-73.

- Peer to Peer Blocking—From the drop-down list, choose **Disable**, **Drop**, or **Forward-Up Stream**.
  - This option allows users to configure peer-to-peer blocking for individual clients rather than universally for all WLAN clients.

Note For controller Release 7.2.x and later, the Forward Up Stream is same as Drop for locally switched clients.

- Wi-Fi Direct Client Policy—Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices might associate with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently. You can use the controller to configure the Wi-Fi Direct Client Policy, on a per-WLAN basis, where you can allow or disallow association of

Wi-Fi devices with infrastructure WLANs, or disable Wi-Fi Direct Client Policy for WLANs altogether. From the Wi-Fi Direct Clients Policy drop-down list, choose one of the following options:

- **Disabled**—Disables the Wi-Fi Direct Clients Policy for the WLAN and deauthenticates all Wi-Fi Direct capable clients.
- **Allow**—Allows the Wi-Fi Direct clients to associate with an infrastructure WLAN.
- **Not-Allow**—Disallows the Wi-Fi Direct clients from associating with an infrastructure WLAN.

Note The Wi-Fi Direct Clients Policy is applicable to WLANs that have APs in local mode only.

Note The Wi-Fi Direct Clients Policy is applicable for controller Release 7.2.x. and later.

- Client Exclusion—Select the check box to enable automatic client exclusion. If it is enabled, set the timeout value in seconds for disabled client machines.
  - Client machines are excluded by MAC address, and their status can be observed.
  - A timeout setting of 0 indicates that administrative control is required to reenable the client.

Note When session timeout is not set, the excluded client remains and does not time out from the excluded state. It does not imply that the exclusion feature is disabled.

- Media Session Snooping—Select the check box to enable media session snooping. This feature enables access points to detect the establishment, termination, and failure of voice calls and then report them to the controller and the NCS. It can be enabled or disabled for each WLAN.

  When media session snooping is enabled, the access point radios advertise this WLAN snoop for Session Initiation Protocol (SIP) voice packets. Any packets destined to or originating from port number 5060 are considered for further inspection. The access point tracks whether Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, already on an active call, or in the process of ending a call and then notify the controller of any major call events.
- KTS based CAC—Select the check box to enable KTS-based CAC support per WLAN.

  WLC supports TSPEC-based CAC and SIP based CAC. But there are certain phones that work with different protocols for CAC, which are based on the Key Telephone System (KTS). For supporting CAC with KTS-based SIP clients, WLC should understand and process the bandwidth request message from those clients, to allocate the required bandwidth on the AP radio, in addition to handling and sending certain other messages, as part of this protocol.

Note The KTS CAC configuration is only supported by Cisco 5508, 7500, WISM2, and 2500 controllers that run controller software Release 7.2.x. This feature is not supported by Cisco 4400 series controllers.

Note The voice parameters appear only if you choose **Platinum (voice)** from the quality of service (QoS) drop-down list on the QoS tab.

- NAC State—From the NAC State drop-down list, choose **SNMP NAC** or **Radius NAC**. SIP errors that are discovered generate traps that appear on the Client Troubleshooting and Alarms pages. The controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing. See the "NAC Integration" section on page 8-44 for more information.

  Note You can enable RADIUS NAC on WLAN with open authentication and MAC filtering. If you are using local web authentication with RADIUS NAC, the Layer 3 web authentication must also be enabled.

- Passive Client—If the check box is selected, it enables passive clients on your WLAN.

  Passive clients are wireless devices like scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information during association with an access point. As a result, when passive clients are used, the controller never knows the IP address unless they use DHCP.

  Wireless LAN controllers currently act as a proxy for ARP requests. On receiving an ARP request, the controller responds with an ARP response instead of passing the request directly to the client. This has two advantages:

  – The upstream device that sends out the ARP request to the client cannot know where the client is located.

  – Reserves power for battery-operated devices like mobile phones and printers as they do not need to respond to every ARP request.

  Because the wireless controller does not have any IP-related information about passive clients, it cannot respond to any ARP requests. The current behavior does not allow the transfer of ARP requests to passive clients. Therefore, any application that tries to access a passive client fails.

  This feature enables ARP requests and responses to be exchanged between wired and wireless clients on a per VLAN/WLAN basis. This feature enables the user to mark a desired WLAN for presence of proxy ARP thereby enabling the controller to pass the ARP requests until the client gets to RUN state.

  Note This feature is supported only on the 5500 and 2100 series controllers.

- DTIM Period (in beacon intervals)—For 802.11a/n and 802.11b/g/n, specify the frequency of the DTIM packet sent in the wireless medium. This period can be configured for every WLAN (except guest WLAN) on all Version 6.0 and later controllers.
- DHCP
  – DHCP Server—Select the check box to override the DHCP server, and enter the IP address of the DHCP server.

    Note For some WLAN configurations, this setting is required.

  – DHCP Addr. Assignment—If you select the **Required** check box, clients connected to this WLAN get an IP address from the default DHCP server.
- Management Frame Protection (MFP)

- MFP Signature Generation—If the check box is selected, it enables signature generation for the 802.11 management frames transmitted by an access point associated with this WLAN. With signature generation, changes to the transmitted management frames by an intruder are detected and reported.
- MFP Client Protection—From the drop-down list, choose **Enabled**, **Disabled**, or **Required** for individual WLAN configurations.

Note The **Enabled** parameter is the same as the **Optional** parameter that you choose from the MFP Client Protection drop-down list in the WLC graphical user interface.

- MFP Version—Displays the Management Frame Protection version.

Note Client-side MFP is available only for those WLANs configured to support CCXv5 (or later) clients. In addition, WPA1 must first be configured.

- Foreign Controller Mapping—Click this link to configure foreign controller mappings. This takes you to the Foreign Controller configuration page. In this configuration page, choose a foreign controller from the Foreign Controller drop-down list and choose an interface or interface group from the Interface/Interface Group drop-down list. After choosing the required options, click **Add** to complete the adding of a foreign controller.
- Client Profiling—Select the check box to enable or disable profiling of all the clients that are associated with the WLAN.

Note Client Profiling is not supported with FlexConnect local authentication.

Note Client Profiling is configurable only when you select the **DHCP Address Assignment** check box.

Note Client profiling is supported for controllers Release 7.2.x.

Adding a WLAN

To add a WLAN, follow these steps:

Step 1 Choose **Configure > Controllers**.

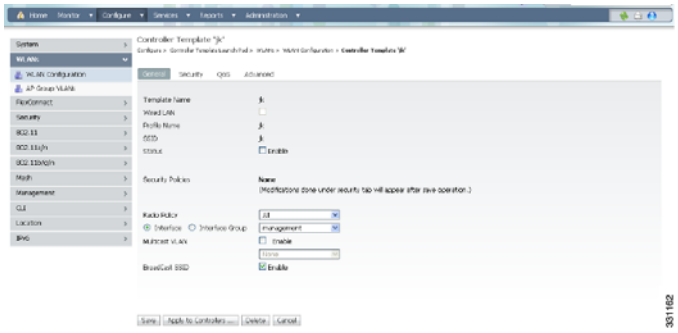
Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, choose **WLANs > WLAN Configuration**.

Step 4 From the Select a command drop-down list, choose **Add a WLAN**.

Step 5 Click **Go** to open the WLAN Details: Add from Template page (see Figure 8-8).

Figure 8-8 WLAN Details: Add From Template Page



Step 6 Choose a template from the Select a template to apply to this controller drop-down list.

Step 7 Click **Apply**.

Note To create a new template for WLANs, use the click here link in this page, or choose **Configure > Controller Template Launch Pad > WLANs > WLAN**.

Deleting a WLAN

To delete a WLAN, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, choose **WLANs > WLAN Configuration**.

Step 4 Select the check boxes of the WLANs that you want to delete.

Step 5 From the Select a command drop-down list, choose **Delete a WLAN**.

Step 6 Click **Go**.

Step 7 Click **OK** to confirm the deletion.

Managing WLAN Status Schedules

The NCS enables you to change the status of more than one WLAN at a time on a given controller. You can select multiple WLANs and select the date and time for that status change to take place.

To schedule multiple WLANs for a status change, follow these steps:

Step 1 Choose **Configure > Controllers**.

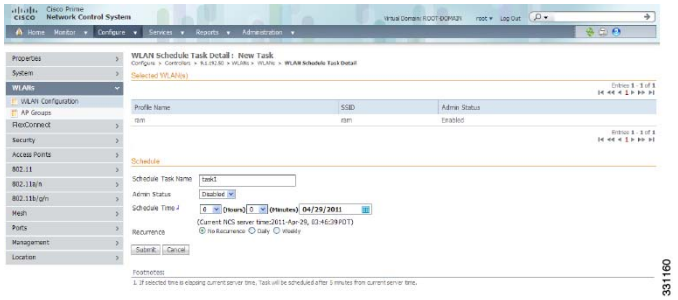
Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, choose **WLANs > WLAN Configuration**.

Step 4 Select the check boxes of the WLANs that you want to schedule for a status change.

Step 5 From the Select a command drop-down list, choose **Schedule Status** to open the WLAN Schedule Task Detail page (see Figure 8-9).

Figure 8-9 WLAN Schedule Task Detail Page



The selected WLANs are listed at the top of the page.

Step 6 Enter a Scheduled Task Name to identify this status change schedule.

Step 7 Choose the new Admin Status (Enabled or Disabled) from the drop-down list.

Step 8 Choose the schedule time using the hours and minutes drop-down lists.

Step 9 Click the calendar icon to choose a schedule date or enter the date in the text box (MM/DD/YYYY).

Step 10 Select the appropriate Recurrence radio button to determine the frequency of the status change (Daily, Weekly, or No Recurrence).

Step 11 Click **Submit** to initiate the status change schedule.

Note For more information on the WLAN Configuration Scheduled Task results, see the "Viewing WLAN Configuration Scheduled Task Results" section on page 8-225.

Mobility Anchors

Mobility anchors are one or more controllers defined as anchors for the WLAN. Clients (802.11 mobile stations such as a laptop) are always attached to one of the anchors.

This feature can be used to restrict a WLAN to a single subnet, regardless of the entry point of the client into the network. In this way, users can access a public or guest WLAN throughout an enterprise but still be restricted to a specific subnet. Guest WLAN can also be used to provide geographical load balancing because WLANs can represent a particular section of a building (such as a lobby, restaurant, and so on).

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the controller is announced to the other controllers in the same mobility group. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EitherIP. The foreign controller decapsulates the packets and forwards them to the client.

Note A 2000 series controller cannot be designated as an anchor for a WLAN. However, a WLAN created on a 2000 series controllers can have a 4100 series controller or a 4400 series controller as its anchor.

Note The L2TP Layer 3 security policies are unavailable for WLANs configured with a mobility anchor.

To view the real time status of mobility anchors for a specific WLAN, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, choose **WLANs > WLAN Configuration**.

Step 4 Click a WLAN ID to view the parameters for a specific WLAN.

Step 5 Click the **Advanced** tab.

Step 6 Click the **Mobility Anchors** link. Table 8-3 describes the parameters that are displayed.

Table 8-3 Mobility Anchors

Field	Description
Mobility Anchor	The IP address of the anchor.
Status	The current status of the anchor. For example, reachable or unreachable.

Configuring WLANs AP Groups

Site-specific VLANs or AP groups limit the broadcast domains to a minimum by segmenting a WLAN into different broadcast domains. Benefits of this include more effective management of load balancing and bandwidth allocation.

To open this page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **WLAN > AP Groups**.

This page displays a summary of the AP groups configured on your network. From here you can add, remove, or view details of an AP group. Click the AP group name on the Access Points tab to view or edit its access point(s). Click the **WLAN Profiles** tab to view, edit, add, or delete WLAN profiles.

Adding Access Point Groups

To add a new access point group, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **WLAN > AP Groups**.

Note AP Groups (for 5.2 and later controllers) is referred to as AP Group VLANs for controllers prior to 5.2.

Step 4 From the Select a command drop-down list, choose **Add AP Groups**.

Step 5 Click **Go**.

In the AP Groups details page, you can add access points and WLAN profiles to this access point group.

Step 6 Enter a name and group description for the access point group.

Note The group description is optional.

Step 7 To add access points to the group, follow these steps:

a. Click the **Access Points** tab.

b. Click **Add**. The access point page displays parameters for available access points. Click the access point name to view or edit parameters for one of the available access points.

c. Select the check box(es) of the access point(s) you want to add.

d. Click **Select**.

Step 8 To add a WLAN profile, click the **WLAN Profiles** tab and configure the following parameters:

a. Click **Add**.

Note To display all available WLAN profile names, delete the current WLAN profile name from the text box. When the current WLAN profile name is deleted from the text box, all available WLAN profiles appear in the drop-down list.

Note Each access point is limited to 16 WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.

Note The WLAN override feature applies only to older controllers that do not support the 512 WLAN feature (can support up to 512 WLAN profiles).

b. Type a WLAN profile name or choose one from the WLAN Profile Name drop-down list.

c. Enter an interface/interface group or choose one from the Interface/Interface Group drop-down list.

Note To display all available interfaces, delete the current interface in the Interface text box. When the current interface is deleted from the Interface text box, all available interfaces appear in the drop-down list.

d. Select the **NAC Override** check box, if applicable. NAC override is disabled by default.

e. When access points and WLAN profiles are added, click **Save**.

Step 9 If you want to add a RF profile, click the **RF Profiles** tab and configure the following parameters:

- 802.11a—Drop-down list from which you can choose an RF profile for APs with 802.11a radios.
- 802.11b—Drop-down list from which you can choose an RF profile for APs with 802.11b radios.
- When RF profiles are added, click **Save**.

Note Use the **Click here** link to add a new RF profile. See the "Configuring RF Profiles Templates (802.11)" section on page 10-92 for more information.

Note Changing the WLAN-interface mapping in an AP Group removes the local VLAN mapping for FlexConnect APs in this group. These mappings need to be reconfigured after applying this change.

Deleting Access Point Groups

To delete an access point group, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **WLAN > AP Groups**.

Step 4 Select the check box(es) of the access point group(s) that you want to delete.

Step 5 From the Select a command drop-down list, choose **Delete AP Groups**.

Step 6 Click **OK** to confirm the deletion.

Auditing Access Point Groups

You can audit the access point group to determine if the NCS and device values differ.

To audit an access point group, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **WLAN > AP Groups**.

Step 4 Click the name of the access point group that you want to audit.

Note Click **Audit** located at the bottom of the page.

Configuring FlexConnect Parameters

FlexConnect enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. There is no deployment restriction on the number of FlexConnect access points per location. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller.

- Configuring FlexConnect AP Groups, page 8-82
- Auditing a FlexConnect Group, page 8-85

Configuring FlexConnect AP Groups

To view a list of existing FlexConnect AP groups, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **FlexConnect > FlexConnect AP Groups**. The FlexConnect AP Groups page opens.

- Group Name—The name of the FlexConnect AP group. Click the group name to view its details.

Note Use the check box to select a group for deletion.

Configuring a FlexConnect AP Group

To configure a FlexConnect access point group, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **FlexConnect > FlexConnect AP Groups**.

Step 4 From the Select a command drop-down list, click **Add FlexConnect AP Group** to open the FlexConnect AP Group > Add From Template pane.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 Click **Apply**.

Note To make modifications to an existing FlexConnect AP Group, click the existing group in the Group Name column of the FlexConnect AP Group page.
To delete an existing group, select the check box of the group you want to remove, and choose **Delete FlexConnect AP Group** from the Select a command drop-down list.

Step 7 Configure the following FlexConnect AP Group parameters:

- General tab
  - Template Name—The name of the template applied to this controller.
  - Primary Radius—From the drop-down list, choose the primary radius authentication server present on the controller.

    Note If a RADIUS authentication server is not present on the controller, the NCS configured RADIUS server does not apply.

    Note You must configure the RADIUS server configuration on the controller before you apply FlexConnect RADIUS server configuration from the NCS.

  - Secondary Radius—From the drop-down list, choose the secondary radius authentication server present on the controller.

    Note If a RADIUS authentication server is not present on the controller, the NCS configured RADIUS server does not apply.

- FlexConnect AP tab
  - Ethernet MAC—Select the check box to apply to the FlexConnect group.

Note An AP Ethernet MAC address cannot exist in more than one FlexConnect group on the same controller. The controller does not allow you to set an AP Ethernet MAC in a FlexConnect group if it is already present in another FlexConnect group.

– Add AP—Click to add an additional FlexConnect AP (present in the NCS) to an existing FlexConnect group. When you click Add AP, only those access points that are part of this FlexConnect group is listed.

Step 8 If you want to enable local authentication for a FlexConnect group, click the **FlexConnect Configuration** tab.

Note Make sure that the Primary RADIUS Server and Secondary RADIUS Server parameters are set to **None** on the General tab.

Step 9 Select the **FlexConnect Local Authentication Enable** check box to enable local authentication for this FlexConnect group. The default value is unselected.

Step 10 To allow a FlexConnect access point to authenticate clients using LEAP, select the **LEAP** check box. Otherwise, to allow a FlexConnect access point to authenticate clients using EAP-FAST, select the **EAP-FAST** check box.

If you have selected the **EAP-FAST** check box, then you are required to provide the EAP-FAST key as well as confirm the EAP-FAST key.

Step 11 Perform one of the following, depending on how you want Protected Access Credentials (PACs) to be provisioned:

- To use manual PAC provisioning, enter the key used to encrypt and decrypt PACs in the EAP=FAST Key text box. The key must be 32 hexadecimal characters.
- To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select the **Ignore Server Key** check box.

Step 12 In the EAP-FAST Authority ID text box, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.

Step 13 In the EAP-FAST Authority Info text box, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.

Step 14 In the EAP-FAST PAC Timeout text box, specify a PAC timeout value by entering the number of seconds for the PAC to remain visible in the edit text box. The valid range is 2 to 4095 seconds.

Note To see if an individual access point belongs to a FlexConnect group, click the **Users configured in the group** link. It advances you to the FlexConnect AP Group page which shows the names of the groups and the access points that belong in it.

Step 15 Click the **Image Upgrade** tab and configure the following:

- FlexConnect AP Upgrade—Select the check box if you want to upgrade the FlexConnect access points.
- Slave Maximum Retry Count—Specify the maximum retries for the slave to undertake to start the download from the master in the FlexConnect group. This option is available only if you select the **FlexConnect AP Upgrade** check box.

Note You are allowed to add an access point as a master access point only if FlexConnect AP Upgrade check box is enabled on the General tab.

Step 16 Click the **VLAN-ACL Mapping** tab to view, add, edit, or remove a VLAN ACL mapping.

a. Click **Add**.

b. Enter a VLAN ID. The valid VLAN ID range is 1—4094.

c. From the Ingress ACL drop-down list, choose an Ingress ACL.

d. From the Egress AC drop-down list, choose an Egress ACL.

e. Click **Save**.

Step 17 Click the **WLAN-ACL Mapping** tab, and select the FlexConnect access control list for external web authentication.

a. Click **Add**.

b. From the WLAN Profile Name drop-down list, choose a WLAN profile.

c. From the WebAuth ACL drop-down list, choose a WebAuth ACL.

d. Click **Save**.

Note You can add up to a maximum of 16 WebAuth ACLs.

Step 18 Click the **WebPolicy ACL** tab and select the FlexConnect access control list to be added as a web policy.

a. Click **Add**.

b. From the Web-Policy ACL drop-down list, choose a WebPolicy ACL.

c. Click **Save**.

Note You can add up to a maximum of 16 Web-Policy ACLs.

Step 19 Click **Save**.

Auditing a FlexConnect Group

If the FlexConnect configuration changes over a period of time either on the NCS or the controller, you can audit the configuration. The changes are visible in subsequent pages. You can specify to refresh the NCS or the controller to synchronize the configuration.

Configuring Security Parameters

This section contains the following topics:

Configuring Controller File Encryption

To configure a controller file encryption, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > File Encryption**. File encryption ensures that data is encrypted when you upload or download the controller configuration file from a TFTP server.

File Encryption parameters include the following:

- File Encryption—If this option is enabled, the data in the controller configuration file is encrypted when it is uploaded or downloaded through the TFTP server.
- Encryption Key—A text string of exactly 16 characters.
- Confirm Encryption Key—Enter the encryption key.

Configuring Controllers > *IPaddr* > Security > AAA

This section describes how to configure controller security AAA parameters and contains the following topics:

Configuring AAA General Parameters

The General page allows you to configure the local database entries on a controller.

To configure the local database entries, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > General**.

Step 4 Enter the maximum number of allowed database entries. This amount becomes effective on the next reboot. The valid range is 512 - 2048.

Configuring AAA RADIUS Auth Servers

To view a summary of existing RADIUS authentication servers, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > RADIUS Auth Servers**. The following RADIUS Auth Servers parameters appear:

- Server Index—Access priority number for the RADIUS server (display only). Click to go to Configure IPaddr > RADIUS Authentication Server.
- Server Address—IP address of the RADIUS server (read-only).
- Port Number—Controller port number (read-only).
- Admin Status—Enable or Disable.
- Network User—Enable or Disable.
- Management User—Enable or Disable.

Adding an Authentication Server

To add an authentication server, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > RADIUS Auth Servers**.

Step 4 From the Select a command drop-down list, choose **Add Auth Server** to open the Radius Authentication Server > Add From Template page.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 Click **Apply**.

Note To create a new template for Radius authentication servers, choose **Configure > Controller Templates > Security > RADIUS Auth Servers**.

Configuring AAA RADIUS Acct Servers

To view a summary of existing RADIUS accounting servers, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > RADIUS Acct Servers**. RADIUS Acct Server parameters include the following:

- Server Index—Access priority number for the RADIUS server (read-only). Click to open the Radius Acct Servers Details page.

  Note To edit or audit the current accounting server parameters, click the Server Index for the applicable accounting server.

- Server Address—IP address of the RADIUS server (read-only).
- Port Number—Controller port number (read-only).
- Admin Status—Enable or Disable.
- Network User—Enable or Disable.

Command Buttons

- Save
- Audit

Adding an Accounting Server

To add an accounting server, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > RADIUS Acct Servers**.

Step 4 From the Select a command drop-down list, choose **Add Acct Server** to open the Radius Acct Servers Details > Add From Template page.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 From the drop-down list, choose a controller to apply to this template.

Step 7 Click **Apply**.

Note To create a new template for Radius accounting servers, choose **Configure > Controller Templates Launch Pad > Security > RADIUS Acct Servers**.

Deleting an Accounting Server

To delete an accounting server, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > RADIUS Acct Servers**.

Step 4 Select the check box(es) for the applicable accounting server(s).

Step 5 From the Select a command drop-down list, choose **Delete Acct Server**.

Step 6 Click **Go**.

Step 7 Click **OK** in the pop-up dialog box to confirm the deletion.

Configuring AAA RADIUS Fallback Parameters

To configure RADIUS fallback parameters, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > RADIUS Fallback**.

Step 4 Add or modify the following parameters:

- RADIUS FallbackMode
- Username
- Time Interval

Step 5 Click **Save**.

Note Click **Audit** to check the present configuration status of the NCS and controller.

Configuring AAA LDAP Servers

This page enables you to add and delete LDAP servers to this controller.

To access the LDAP Servers page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > LDAP Servers**.

This page displays LDAP servers currently used by this controller and contains the following parameters:

- Check box—Select the check box to choose an LDAP server for deletion.
- Server Index—A number assigned to identify the LDAP server.

Note Click the index number to go the LDAP server configuration page.

- Server Address—The LDAP server IP address.
- Port Number—The port number used to communicate with the LDAP server.
- Admin Status—Server template status.

  Indicates if use of the LDAP server template is enabled o disabled.

Note If the title of a column is a link, click it to toggle between ascending and descending order.

Note The NCS now supports LDAP configuration for both an anonymous or authenticated bind. For more information, see the "Configuring New LDAP Bind Requests" section on page 8-91.

LDAP Servers Select a command Drop-Down List Options

Adding LDAP Server

To add a LDAP Server, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > LDAP Servers**.

Step 4 From the Select a command drop-down list, choose **Add LDAP Server**.

Step 5 Click **Go**.

Deleting LDAP Servers

To delete the LDAP Server, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > LDAP Servers**.

Step 4 Select the check box(es) of the LDAP servers that you want to delete.

Step 5 From the Select a command drop-down list, choose **Delete LDAP Servers**.

Step 6 Click **Go**.

Configuring New LDAP Bind Requests

The NCS now supports LDAP configuration for both an anonymous or authenticated bind. A bind is a socket opening that performs a lookup.

To configure LDAP bind requests, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 From the left sidebar menu, choose **Security > AAA > LDAP Servers**.

Step 3 From the Bind Type drop-down list, choose **Authenticated** or **Anonymous**. If you choose Authenticated, you must enter a bind username and password as well.

Step 4 In the Server User Base DN text box, enter the distinguished name of the subtree in the LDAP server that contains a list of all the users.

Step 5 In the Server User Attribute text box, enter the attribute that contains the username in the LDAP server.

Step 6 In the Server User Type text box, enter the ObjectType attribute that identifies the user.

Step 7 In the Retransmit Timeout text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

Step 8 Select the **Admin Status** check box if you want the LDAP server to have administrative privileges.

Step 9 Click **Save**.

Configuring AAA TACACS+ Servers

This page enables you to add and delete TACACS+ servers to this controller.

To access the TACACS+ Servers page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > TACACS+ Servers**.

This page displays TACACS+ servers currently used by this controller and contains the following parameters:

- Check box—Select the check box to choose a TACACS+ server for deletion.
- Server Type—The TACACS+ server type—accounting, authorization, or authentication.
- Server Index—A number assigned to identify the TACACS+ server and set its use priority. Click the index number to go the TACACS+ server configuration page.
- Server Address—The TACACS+ server IP address.
- Port Number—The port number used to communicate with the TACACS+ server.
- Admin Status—Server template status.

  Indicates if use of the TACACS+ server template is enabled.

If the title of a column is a link, click it to toggle between ascending and descending order.

The Select a command drop-down list has the following options:

- Add TACACS+ Server—Choose this option, then click **Go** to add a TACACS+ server to the controller.
- Delete TACACS+ Servers—Choose this option, then click **Go** to delete all TACACS+ servers with a selected check box from the controller.

Configuring AAA Local Net Users

This page provides a summary of the existing local network user controllers for clients who are allowed to access a specific WLAN. This is an administrative bypass of the RADIUS authentication process. Layer 3 Web Authentication must be enabled. The client information is passed to the RADIUS authentication server first, and if the client information does not match a RADIUS database entry, this local database is polled. Clients located in this database are granted access to network services if the RADIUS authentication fails or does not exist.

- Adding a Local Net User, page 8-92
- Deleting a Local Net User, page 8-93

To view existing local network users, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > Local Net Users**. The Local Net Users page displays the following local net user parameters:

- Username—User-defined identification.
- WLAN ID—Any WLAN ID, 1 through 16; 0 for all WLANs; 17 for third-party WLAN that this local net user is allowed to access.
- Description—Optional user-defined description.

Adding a Local Net User

To add a local net user, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > Local Net Users**.

Step 4 From the Select a command drop-down list, choose **Add Local Net User** to open the **Local Net User > Add From Template** page.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 Click **Apply**.

Note To create a new template for local net users, choose **Configure > Controller Templates > Security > Local Net Users**. See the "Configuring a Local Network Users Template" section on page 10-59 for more information.

Deleting a Local Net User

To delete a local net user, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > Local Net Users**.

Step 4 Select the check box(es) for the applicable local net user(s).

Step 5 From the Select a command drop-down list, choose **Delete Local Net Users**.

Step 6 Click **Go**.

Step 7 Click **OK** in the dialog box to confirm the deletion.

Configuring AAA MAC Filtering

This page enables you to view MAC Filter information.

Note You cannot use MAC address in the broadcast range.

To access the MAC Filtering page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > MAC Filtering**. The MAC Filtering page displays the following parameters:

- MAC Filter Parameters
  - RADIUS Compatibility Mode—User-defined RADIUS server compatibility: Cisco ACS, FreeRADIUS, or Other.

  - MAC Delimiter—The MAC delimiters can be Colon (xx:xx:xx:xx:xx:xx), Hyphen (xx-xx-xx-xx-xx-xx), Single Hyphen (xxxxxx-xxxxxx), or No Delimiter (xxxxxxxxxxxx), as required by the RADIUS server.
- MAC Filters
  - MAC Address—Client MAC address. Click to open Configure *IPaddr* > MAC Filter.
  - WLAN ID—1 through 16, 17 = Third-party AP WLAN, or 0 = all WLANs.
  - Interface—Displays the associated Interface Name.
  - Description—Displays an optional user-defined description.

Step 4 From the Select a command drop-down list, choose **Add MAC Filters** to add a MAC Filter, **Delete MAC Filters** to delete the template(s), or **Edit MAC Filter** Parameters to edit the MAC Filters.

Step 5 Click **Go**.

Configuring AAA AP/MSE Authorization

The AP/MSE Authorization page displays the access point policies and the list of authorized access points along with the type of certificate that an access point uses for authorization.

Note You cannot use MAC address in the broadcast range.

To access the AP/MSE Authorization page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > AP/MSE Authorization**. The AP/MSE Authorization page displays the following parameters:

- AP Policies
  - Authorize APs—Enabled or Disabled.
  - Accept SSC-APs—Enabled or Disabled.
- AP/MSE Authorization
  - AP/MSE Base Radio MAC Address—The MAC address of the authorized access point.

    Note Click the AP/MSE Base Radio MAC Address to view AP/MSE Authorization details.

  - Type
  - Certificate Type—MIC or SSC.
  - Key Hash—The 40-hex long SHA1 key hash.

    Note The key hash is displayed only if the certificate type is SSC.

Command Buttons

- Add AP/MSE Auth Entry—Select this command, and click **Go**. See the "Configuring an Access Point or MSE Authorization Template" section on page 10-63.
- Delete AP/MSE Auth Entries—Select one or more access points, select this command, and click **Go** to delete the selected access point from the AP authorization list.
- Edit AP Policies—Select this command, and click **Go**. See the "Editing AP Policies" section on page 8-95.

Editing AP Policies

To edit AP/MSE Authorization access point policies, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > AP/MSE Authorization**.

Step 4 In Edit AP Policies page, edit the following parameters, if necessary:

- Authorize APs—Select the check box to enable access point authorization.
- Accept SSC-APs—Select the check box to enable the acceptance of SSE access points.

Step 5 Click **Save** to confirm the changes, **Audit** to perform an audit on these device values, or **Cancel** to close this page with no changes.

Configuring AAA Web Auth Configuration

The Web Auth Configuration page enables the user to configure the web auth configuration type. If the type is configured as customized, the user downloaded web auth replaces the controller-provided internal web auth page.

To access the Web Auth Configuration page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > Web Auth Configuration**.

Step 4 In the Web Authentication page, choose the Web Auth Type from the drop-down list. Web auth options include a default internal web page, a customized web authentication page, or an external web page.

Step 5 Configure the web auth parameters depending on the type chosen:

- Default Internal
  - Logo Display—Enable or disable logo display.
  - Web Auth Page Title—Title displayed on web authentication page.
  - Web Auth Page Message—Message displayed on web authentication page.
  - Custom Redirect URL—URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page.

- Customized Web Auth

  You have the option of downloading an example login page and customizing the page. If you are using a customized web authentication page, it is necessary to download the example login.tar bundle file from the server, edit the login.html file and save it as either a .tar or .zip file, then download the .tar or .zip file to the controller.

  Click the preview image to download this sample login page as a TAR. After editing the HTML you might click here to redirect to the Download Web Auth page. See the "Downloading a Customized WebAuthentication Bundle to a Controller" section on page 8-16 for more information.

- External
  - External Redirect URL—Location of the login.html on an external server on the network.

    If there are not any external web auth servers configured, you have the option of configuring one.

    No external Web Auth Server(s) configured. Choose this option to configure external web auth servers.

Note To configure an external web server template, see the "Configuring an External Web Auth Server Template" section on page 10-71.

Command Buttons

- Save—Save the current settings to the controller.
- Audit—Check the present configuration status of the NCS and controller.

Configuring AAA Password Policy

This page enables you to determine your password policy.

To make modifications to an existing password policy, follow these steps:

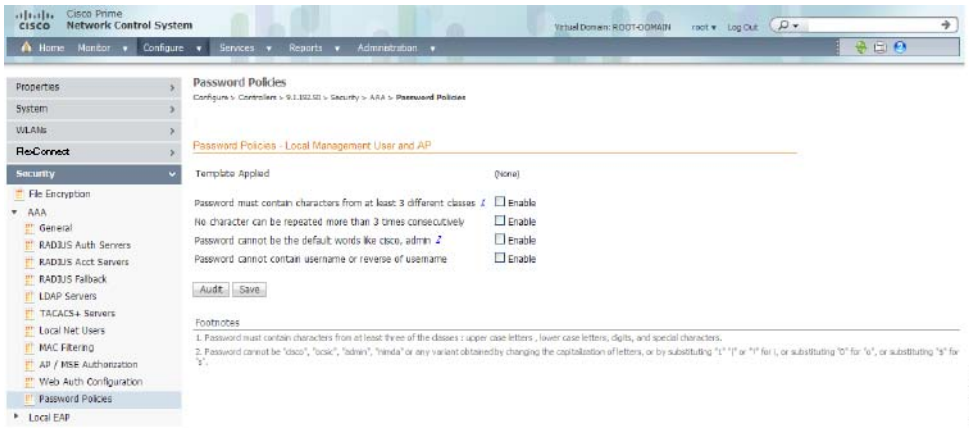
Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > Password Policy**.

Step 4 Modify the password policy parameters as appropriate (see Figure 8-10).

Figure 8-10 Password Policy



Step 5 Click **Save**.

Note If you disable password policy options, you see a "Disabling the strong password check(s) will be a security risk as it allows weak passwords" message.

Configuring Controllers > *IPaddr* > Security > Local EAP

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down.

When you enable local EAP, the controller serves as the authentication server and the local user database, making it independent of an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users.

Configuring Local EAP General Parameters

This page allows you to specify a timeout value for local EAP. You can then add a template with this timeout value or make changes to an existing template.

Note If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

To specify a timeout value for local EAP, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > Local EAP > General - Local EAP**.

Step 4 Enter the Local Auth Active Timeout in the Local Auth Active Timeout text box (in seconds).

Note Local Auth Active Timeout refers to the timeout period during which Local EAP is always used after all Radius servers are failed.

Step 5 The following values should be adjusted if you are using EAP-FAST, manual password entry, one-time password, or 7920/7921 phones.

Note You must increase the 802.1x timeout values on the controller (default=2 seconds) for the client to obtain the PAC using automatic provisioning. We recommend the default timeout on the Cisco ACS server of 20 seconds.

- Local EAP Identify Request Timeout =1 (in seconds)
- Local EAP Identity Request Maximum Retries=20 (in seconds)
- Local EAP Dynamic Wep Key Index=0
- Local EAP Request Timeout=20 (in seconds)
- Local EAP Request Maximum Retries=2
- EAPOL-Key Timeout=1000 (in milli-seconds)
- EAPOL-Key Max Retries=2
- Max-Login Ignore Identity Response

Note Roaming fails if these values are not set the same across multiple controllers.

Step 6 Click **Save**.

Command Buttons

- Save—Click to save the current template.
- Apply to Controllers—Click to apply the current template to controllers. In the Apply to Controllers page, choose the applicable controllers, and click **OK**.
- Delete—Click to delete the current template. If the template is currently applied to controllers, click **OK** to confirm that you want to remove the template from the selected controllers to which it is applied.
- Cancel—Click to cancel the current template creation or changes to the current template.

Configuring Local EAP Profiles

This page allows you to apply a template for a local EAP profile or make modifications to an existing template.

Note The LDAP backend database supports only these local EAP methods: EAP-TLS and EAP-FAST with certificates. LEAP and EAP-FAST with PACs are not supported for use with the LDAP backend database.

- Viewing Existing Local EAP Profiles, page 8-99
- Adding a Local Net User, page 8-99

Viewing Existing Local EAP Profiles

To view existing local EAP profiles, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > Local EAP > Local EAP Profiles**. The Local EAP Profiles page displays the following parameters:

- EAP Profile Name—User-defined identification.
- LEAP—Authentication type that leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. A username and password are used to perform mutual authentication with the RADIUS server through the access point.
- EAP-FAST—Authentication type (Flexible Authentication via Secure Tunneling) that uses a three-phased tunnel authentication process to provide advanced 802.1x EAP mutual authentication. A username, password, and PAC (protected access credential) are used to perform mutual authentication with the RADIUS server through the access point.
- TLS—Authentication type that uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It requires a client certificate for authentication.
- PEAP—Protected Extensible Authentication Protocol.

Adding a Local Net User

To add a local EAP profile, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > Local EAP > Local EAP Profile**.

Step 4 From the **Select a command** drop-down list, choose **Add Local EAP Profile** to open the Local EAP Profile > Add From Template page.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 Click **Apply**.

Note To create a new template for local EAP profiles, choose **Configure > Controller Templates > Security > Local EAP Profiles**.

Configuring Local EAP General EAP-FAST Parameters

This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1x EAP mutual authentication. A username, password, and PAC are used to perform mutual authentication with the RADIUS server through the access point.

To set EAP-FAST Parameters, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > Local EAP > EAP-FAST Parameters**.

Step 4 Enter the following parameters:

- Time to live for the PAC—The number of days for the PAC to remain viable. The valid range is 1 to 1000 days; the default setting is ten days.
- Authority ID—The authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters but it must be an even number of characters.
- Authority Info—The authority identifier of the local EAP-FAST server in text format.
- Server Key—The key (in hexadecimal characters) used to encrypt and decrypt PACs.
- Confirm Server Key—Verify the correct Server Key by re-typing it.
- Anonymous Provision—Select the check box to enable anonymous provisioning.

Note This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If this feature is disabled, PACs must be manually provisioned.

Step 5 Click **Save**.

Configuring Local EAP General Network Users Priority

To specify the order that LDAP and local databases use to retrieve user credential information, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > Local EAP > Network Users Priority**.

Step 4 Use the left and right pointing arrows to include or exclude network credentials in the right-most list.

Step 5 Use the up and down buttons to determine the order credentials are attempted.

Step 6 Click **Save**.

Configuring User Login Policies

To configure the user login policies, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > User Login Policies**.

Step 4 Enter the maximum number of concurrent logins allowed for a single username.

Step 5 Click **Save**.

Managing Manually Disabled Clients

The Disabled Clients page enables you to view excluded (blacklisted) client information.

Clients who fail to authenticate three times when attempting to associate are automatically blocked, or excluded, from further association attempts for an operator-defined timeout. After the Excluded timeout, the client is allowed to retry authentication until it associates or fails authentication and is excluded again.

Note You cannot use MAC address in the broadcast range.

To access the Manually Disabled Clients page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > Manually Disabled Clients**. The Manually Disabled Clients page displays the following parameters:

- MAC Address—Disabled Client MAC addresses. Click a list item to edit the disabled client description.
- Description—Optional description of disabled client.

Manually Disabled Clients Select a command Drop-Down List Options

- Add Manually Disabled Client—Choose this option from the drop-down list, and click **Go**. See the "Configuring a Manually Disabled Client Template" section on page 10-64.
- Delete Manually Disabled Clients—Select the applicable controller check box, choose this option from the drop-down list, and click **Go**.

Configuring Access Control Lists

The Access Control Lists page displays access control lists (ACLs) available for this controller. It also enables you to add a new rule or edit an existing rule in an applied access control list.

To access the Access Control Lists page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the applicable IP address in the IP Address column.

Step 3 From the left sidebar menu, choose **Security > Access Control Lists**.

- Check box—Use the check box to select one or more ACLs for deletion.
- ACL Name—User-defined name of this template. Click an ACL item to view its parameters. See the "Configuring IPaddr > Access Control List > listname Rules" section on page 8-102.

Configuring *IPaddr* > Access Control List > *listname* Rules

This page displays current access control list (ACL) rules applied to this access control list.

To access the Access Control Lists Rules page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the applicable IP address in the IP address column.

Step 3 From the left sidebar menu, choose **Security > Access Control Lists**.

Step 4 Click an ACL name.

- Check box—Select to delete access control list rules.
- Seq#—The operator can define up to 64 Rules for each ACL. The Rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if Rules 1 through 4 are already defined and you add Rule 29, it is added as Rule 5.

Note If you add or change a Sequence number, operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have Sequence numbers 1 through 7 defined and change number 7 to 5, operating system automatically reassigns Sequence 6 to 7 and Sequence 5 to 6.

- Action—Permit, Deny.
- Source IP/Mask—Source IP address and mask.
- Destination IP/Mask—Destination IP address and mask.
- Protocol—Protocol to use for this ACL:
  - Any—All protocols
  - TCP—Transmission Control Protocol
  - UDP—User Datagram Protocol
  - ICMP—Internet Control Message Protocol
  - ESP—IP Encapsulating Security Payload

  - AH—Authentication Header
  - GRE—Generic Routing Encapsulation
  - IP—Internet Protocol
  - Eth Over IP—Ethernet over Internet Protocol
  - Other Port OSPF—Open Shortest Path First
  - Other—Any other IANA protocol (http://www.iana.org/)

  If TCP or UDP is selected, Source Port and Dest Port parameters appear:

  - Source Port—Source Port. Can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
  - Dest Port—Destination port. If TCP or UDP is selected, can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.

- DSCP (Differentiated Services Code Point)—Any, or 0 through 255.
- Direction—Any, Inbound (from client) or Outbound (to client).

To add a new ACL rule, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Access Control Lists**.

Step 4 Click an ACL name.

Step 5 Click an applicable Seq#, or choose **Add New Rule** to access this page.

Configuring FlexConnect Access Control Lists

The ACLs on FlexConnect provide a mechanism to cater to the need for access control at the FlexConnect access point for protection and integrity of locally switched data traffic from the access point.

This section contains the following topics:

- Adding a FlexConnect Access Control List, page 8-103
- Deleting a FlexConnect Access Control List, page 8-104

Adding a FlexConnect Access Control List

To add an Access Control List for FlexConnect access points, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **Security > FlexConnect ACLs**.

Step 4 From the Select a command drop-down list, choose **Add FlexConnect ACLs**.

Step 5 Click **Go**.

Note You cannot add a FlexConnect ACL if there is no template created. If you try to create an FlexConnect ACL when there are no templates available, you are redirected to the New Controller Templates page where you can create a template for FlexConnect ACL.

The FlexConnect ACLs Details page appears.

Step 6 Choose a template from the drop-down list to apply to the controller, and click **Apply**.

The FlexConnect ACL that you created appears in Configure > Controllers > *IP Address* > Security > FlexConnect ACLs.

Deleting a FlexConnect Access Control List

To delete a FlexConnect ACL, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **Security > FlexConnect ACLs**.

Step 4 From the FlexConnect ACLs page, select one or more FlexConnect ACLs to delete.

Step 5 From the Select a command drop-down list, choose **Delete FlexConnect ACLs**.

Step 6 Click **Go**.

Configuring CPU Access Control Lists

Access control lists (ACLs) can be applied to the controller CPU to control traffic to the CPU.

The Access Control Lists Rules page displays the name of the CPU access control list template applied to the chosen controller.

To access the Access Control Lists Rules page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **Security > CPU Access Control Lists**.

Step 4 Select the **Enable CPU ACL** check box to enable the CPU ACL.

If this check box is selected, the following parameters are available:

- ACL Name—Choose the ACL to use from the ACL Name drop-down list.
- CPU ACL Mode—Choose which data traffic direction this CPU ACL list controls.

The choices include: **The wired side of the data traffic**, **the wireless side of the data traffic**, or **both wired and wireless**.

Configuring the IDS Sensor List

When the sensors identify an attack, they alert the controller to shun the offending client. When you add a new IDS (Intrusion Detection System) sensor, you register the controller with that IDS sensor so that the sensor can send shunned client reports to the controller. The controller also polls the sensor periodically.

To view IDS sensors, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > IDS Sensor Lists**.

The IDS Sensor page lists all IDS sensors that have been configured for this controller. Click an IP address to view details for a specific IDS sensor.

Configuring CA Certificates

A CA certificate is a digital certificate issued by one certificate authority (CA) for another certification CA.

- Importing a CA Certificate, page 8-105
- Pasting a CA Certificate Directly, page 8-105

Importing a CA Certificate

To import a CA certificate from a file, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > IP Sec Certificates > CA Certificate**.

Step 4 Click **Browse** to navigate to the applicable certificate file.

Step 5 Click **Open**.

Step 6 Click **Save**.

Pasting a CA Certificate Directly

To paste a CA certificate directly, follow these steps:

Step 1 Copy the CA certificate to your computer clipboard.

Step 2 Choose **Configure > Controllers**.

Step 3 Click an applicable IP address.

Step 4 From the left sidebar menu, choose **Security > IP Sec Certificates > CA Certificate**.

Step 5 Select the **Paste** check box.

Step 6 Paste the certificate directly into the text box.

Step 7 Click **Save**.

Configuring ID Certificates

This page lists the existing network ID certificates by certificate name. An ID certificate can be used by web server operators to ensure secure server operation. This section contains the following topics:

- Importing an ID Certificate, page 8-106
- Pasting an ID Certificate, page 8-106

Importing an ID Certificate

To import an ID certificate from a file, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > IP Sec Certificates > ID Certificate**.

Step 4 From the Select a command drop-down list, choose **Add Certificate**.

Step 5 Click **Go**.

Step 6 Enter the Name and Password.

Step 7 Click **Browse** to navigate to the applicable certificate file.

Step 8 Click **Open**.

Step 9 Click **Save**.

Pasting an ID Certificate

To paste an ID certificate directly, follow these steps:

Step 1 Copy the ID certificate to your computer clipboard.

Step 2 Choose **Configure > Controllers**.

Step 3 Click an applicable IP address.

Step 4 From the left sidebar menu, choose **Security > IP Sec Certificates > ID Certificate**.

Step 5 From the Select a command drop-down list, choose **Add Certificate**.

Step 6 Click **Go**.

Step 7 Enter the Name and Password.

Step 8 Select the **Paste** check box.

Step 9 Paste the certificate directly into the text box.

Step 10 Click **Save**.

Note ID certificates are available only if the controller is running Cisco Unified Wireless Network Software Version 3.2 or higher.

Note To delete a certificate, select it, choose **Delete Certificates** from the Select a command drop-down list, and click **Go**.

Configuring Controllers > *IPaddr* > Security > Web Auth Certificate

This page enables you to download a web authorization certificate or regenerate the internally-generated web auth certificate.

To access the Web Auth Certificate page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Web Auth Certificate**.

Caution Each certificate has a variable-length embedded RSA Key. The RSA key can vary from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a certificate authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 Bits.

- Download Web Auth Certificate—Click to access the Download Web Auth Certificate to Controller page. See the "Downloading Web Auth or Web Admin Certificate to the Controller" section on page 8-155 for additional information.

Command Buttons

- Regenerate Cert—Regenerate the internally-generated web auth certificate.

Configuring Wireless Protection Policies

This section describes the wireless protection policy configurations and contains the following topics:

- Configuring Custom Signatures, page 8-114
- Configuring AP Authentication and MFP, page 8-114

Configuring Rogue Policies

This page enables you to set up policies for rogue access points.

To access the Rogue Policies page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > Rogue Policies**. The following parameters appear:

- Rogue Location Discovery Protocol—RLDP determines whether or not the rogue is connected to the enterprise wired network. Choose one of the following from the drop-down list:
  - Disable—Disables RLDP on all access points. This is the default value.
  - All APs—Enables RLDP on all access points.
  - Monitor Mode APs—Enables RLDP only on access points in monitor mode.

Note Make sure that rogue detection is enabled on the desired access points. Rogue detection is enabled by default for all access points joined to a controller (except for OfficeExtend access points). However, in the NCS software Release 6.0 or later, you can enable or disable rogue detection for individual access points by selecting or unselecting the **Rogue Detection** check box in the Access Point Details page. See the "Configuring Access Points" section on page 8-161 for more information.

Note Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

- Rogue APs
  - Expiration Timeout for Rogue AP and Rogue Client Entries (seconds)—Enter the number of seconds after which the rogue access point and client entries expire and are removed from the list.

    The valid range is 240 to 3600 seconds and the default value is 1200 seconds.

    Note If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for any classification type.

  - Rogue Detection Report Interval—Enter the time interval in seconds at which the APs should send the rogue detection report to the controller. Valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.
  - Rogue Detection Minimum RSSI—Enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. Valid range is -70 dBm to -128 dBm, and the default value is -128 dBm. This feature is applicable to all the AP modes.

Note There can be many rogues with very weak RSSI values that do not provide any valuable information in the rogue analysis. Therefore, you can use this option to filter the rogues by specifying the minimum RSSI value at which the APs should detect rogues.

  - Rogue Detection Transient Interval—Enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only.

- Rogue Clients
  - Validate rogue clients against AAA—Select the check box to use the AAA server or local database to validate if rogue clients are valid clients. The default value is unselected.
  - Detect and report Adhoc networks—Select the check box to enable ad-hoc rogue detection and reporting. The default value is selected.

Command Buttons

- Save—Save the changes made to the client exclusion policies and return to the previous page.
- Audit—Compare the NCS values with those used on the controller.

Configuring Rogue AP Rules

This page enables you to view and edit current Rogue AP Rules.

To access the Rogue AP Rules page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > Rogue AP Rules**. The Rogue AP Rules displays the Rogue AP Rules, the rule types (Malicious or Friendly), and the rule sequence.

Step 4 Click a Rogue AP Rule to view or edit its details. See the "Configuring a Rogue AP Rules Template" section on page 10-83 for more information.

Configuring Client Exclusion Policies

This page enables you to set, enable, or disable the client exclusion policies applied to the controller.

To access the Client Exclusion Policies page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > Client Exclusion Policies**. The following parameters appear:

- Excessive 802.11a Association Failures—If enabled, clients are excluded on the sixth 802.11 association attempt, after five consecutive failures.
- Excessive 802.11a Authentication Failures—If enabled, clients are excluded on the sixth 802.11 authentication attempt, after five consecutive failures.
- Excessive 802.11x Authentication Failures—If enabled, clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.
- Excessive 802.11 Web Authentication Failures—If enabled, clients are excluded on the fourth web authentication attempt, after three consecutive failures.
- IP Theft Or Reuse—If enabled, clients are excluded if the IP address is already assigned to another device.

Step 4 Click **Save** to save the changes made to the client exclusion policies and return to the previous page or click **Audit** to compare the NCS values with those used on the controller.

Configuring IDS Signatures

You can configure IDS Signatures, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller. If an attack is detected, an appropriate mitigation action is initiated.

Cisco supports 17 standard signatures on the controller as shown on the Standard Signatures and Custom Signatures pages. For more information on these IDS Signatures, see the *Cisco Prime Network Control System Configuration Guide*.

- Configuring Controller Standard Signature Parameters, page 8-110
- Configuring Custom Signatures, page 8-114
- Configuring AP Authentication and MFP, page 8-114

Configuring Controller Standard Signature Parameters

The Standard Signature Parameters page shows the list of Cisco-supplied signatures that are currently on the controller. This section contains the following topics:

- Downloading Signature Files, page 8-111
- Uploading Signature Files, page 8-112
- Global Settings for Standard and Custom Signatures, page 8-113

To access the Standard Signatures page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > Standard Signatures**. This page displays the following parameters:

- Precedence—The order in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. For example:
  - None—No action is taken.
  - Report—Report the detection.
- State—Enabled or Disabled.
- Description—A more detailed description of the type of attack the signature is trying to detect.

Note Click a signature Name to view individual parameters and to enable or disable the signature.

Downloading Signature Files

To download a signature file, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > Standard Signatures** or **Security > Wireless Protection Policies > Custom Signatures**.

Step 4 From the Select a command drop-down list, choose **Download Signature Files**.

Note This function can also be accessed by choosing **System > Commands > Upload/Download Commands > Download IDS Signatures**.

Step 5 Click **Go**.

Step 6 Copy the signature file (*.sig) to the default directory on your TFTP server.

Step 7 Choose **Local Machine** from the File is Located On. If you know the filename and path relative to the server root directory, you can also choose **TFTP server**.

Step 8 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries.

Step 9 Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout.

Step 10 The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** to navigate to it. A "revision" line in the signature file specifies whether the file is a Cisco-provided standard signature file or a site-tailored custom signature file (custom signature files must always have revision=custom).

Note If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried. The local machine option initiates a two-step operation. First, the local file is copied from the administrator workstation to the NCS own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the NCS server TFTP directory, and the downloaded web page now automatically populates the filename.

Step 11 Click **OK**.

Uploading Signature Files

To upload a signature file from the controller, follow these steps:

Step 1 Obtain a signature file from Cisco (hereafter called a standard signature file). You can also create your own signature file (hereafter called a custom signature file) by following the "Downloading Signature Files" section on page 8-111.

Step 2 Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the signature download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port cannot be routed.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port cannot be routed.
- A third-party TFTP server cannot run on the same computer as the NCS because the NCS built-in TFTP server and third-party TFTP server use the same communication port.

Step 3 Choose **Configure > Controllers**.

Step 4 Click an applicable IP address.

Step 5 From the left sidebar menu, choose **Security > Wireless Protection Policies > Standard Signatures** or **Security > Wireless Protection Policies > Custom Signatures**.

Step 6 From the Select a command drop-down list, choose **Upload Signature Files from controller**.

Note This function can also be accessed by choosing **Security > Custom Signatures > Select a command > Upload Signature Files from controller** or **System > Commands > Upload/Download Commands > Upload File from Controller**.

Step 7 Specify the TFTP server name being used for the transfer.

Step 8 If the TFTP server is new, enter the TFTP IP address in the **Server IP Address** field.

Step 9 Choose **Signature Files** from the File Type drop-down list.

Step 10 The signature files are uploaded to the root directory which was configured for use by the TFTP server. You can change to a different directory at the Upload to File field (this field only shows if the Server Name is the default server). The controller uses this local filename as a base name and then adds _std.sig as a suffix for standard signature files and _custom.sig as a suffix for custom signature files.

Step 11 Click **OK**.

Global Settings for Standard and Custom Signatures

This command enables all signatures that were individually selected as enabled. If this text box remains unselected, all files are disabled, even those that were previously enabled. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.

To enable all standard and custom signatures currently on the controller, follow these steps:

Step 1 From the Select a command drop-down list, choose **Edit Signature Parameters**.

Step 2 Click **Go**.

Step 3 Select the **Enable Check for All Standard and Custom Signatures** check box.

Step 4 Click **Save**.

To enable or disable an individual signature, follow these steps:

Step 1 Click an applicable Name for the type of attack you want to enable or disable.

The Standard Signature parameters page shows the list of Cisco-supplied signatures that are currently on the controller. The Custom Signatures page shows the list of customer-supplied signatures that are currently on the controller. The following parameters are displayed in both the signature page and the detailed signature page:

- Precedence—The order, or precedence, in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Description—A more detailed description of the type of attack that the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. One possibility is *None*, where no action is taken, and another is Report, to report the detection.
- Frequency—The signature frequency or the number of matching packets per interval that must be identified at the detecting access point level before an attack is detected. The range is 1 to 32,000 packets per interval and the default value is 50 packets per interval.
- Quiet Time—The length of time (in seconds) after which no attacks have been detected at the individual access point level, and the alarm can stop. This time appears only if the MAC information is all or both. The range is 60 to 32,000 seconds and the default value is 300 seconds.
- MAC Information—Whether the signature is to be tracked per network or per MAC address or both at the detecting access point level.
- MAC Frequency—The signature MAC frequency or the number of matching packets per interval that must be identified at the controller level before an attack is detected. The range is 1 to 32,000 packets per interval and the default value is 30 packets per interval.
- Interval—Enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds and the default value is 1 second.

- Enable—Select this check box to enable this signature to detect security attacks or unselect it to disable this signature.
- Signature Patterns—The pattern that is being used to detect a security attack.

Step 2 From the Enable drop-down list, choose **Yes**. Because you are downloading a customized signature, you should enable the files named with the _custom.sgi and disable the standard signature with the same name but differing suffix. For example, if you are customizing broadcast probe flood, you want to disable broadcast probe flood in the standard signatures but enable it in custom signatures.

Step 3 Click **Save**.

Configuring Custom Signatures

The Custom Signature page shows the list of customer-supplied signatures that are currently on the controller.

For more information on Signatures, see the following sections:

- Downloading Signature Files, page 8-111
- Uploading Signature Files, page 8-112
- Global Settings for Standard and Custom Signatures, page 8-113

To access the Custom Signatures page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > Custom Signatures**. This page displays the following parameters:

- Precedence—The order in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. For example:
  - None—No action is taken.
  - Report—Report the detection.
- State—Enabled or Disabled.
- Description—A more detailed description of the type of attack the signature is trying to detect.

Note Click a signature Name to view individual parameters and to enable or disable the signature.

Configuring AP Authentication and MFP

This page enables you to set the access point authentication policy.

To access the AP Authentication and MFP (Management Frame Protection) page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > AP Authentication and MFP**.

This page displays the following fields:

- RF Network Name—Not an editable text box. The RF Network Name entered in the General parameters page (See Configure *IPaddr* > General) is displayed here.
- Protection Type—From the drop-down list, choose one of the following authentication policies:
  - **None**—No access point authentication policy.
  - **AP Authentication**—Apply authentication policy.
  - **MFP**—Apply Management Frame Protection. See the "Monitoring Management Frame Protection" section on page 5-19 for more information.
- Alarm Trigger Threshold—(Appears only when AP Authentication is selected as the Protection Type). Set the number of hits to be ignored from an alien access point before raising an alarm.

  The valid range is from 1 to 255. The default value is 255.

Command Buttons

- Save
- Audit

Configuring Cisco Access Points

You can use the Configure > Controllers page to view and configure Cisco access points for a specific controller.

To access the Cisco APs page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Access Points > Cisco APs**. The Cisco APs page opens and displays the following parameters:

- AP Name—Click an access point name to view or configure access point details.
- Base Radio MAC
- Admin Status
- AP Mode
- Software Version
- Primary Controller Name

Step 4 Click an access point name to view or configure the access point details. The displayed information might vary depending on the access point type.

Note See the "Configuring Access Points" section on page 8-161 for more detailed information.

Command Buttons

- Save—Save the current settings.
- Audit—Discover the present status of this access point.

Sniffer Feature

When the sniffer feature is enabled on an access point, the access point functions as a sniffer and captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. The packets contain information on timestamp, signal strength, packet size, and so on.

Note The sniffer feature can be enabled only if you are running AiroPeek, which is a third-party network analyzer software that supports decoding of data packets. For more information on AiroPeek, see the following URL: www.wildpackets.com/products/airopeek/overview

Prerequisites for Using the Sniffer Feature

Before using the sniffer feature, you must complete the following:

- Configure an access point in sniffer mode at the remote site. For information on how to configure an access point in sniffer mode, see the "Configuring an AP in Sniffer Mode Using the Web User Interface" section on page 8-117.
- Install AiroPeek Version 2.05 or later on a Windows XP machine.

Note You must be a WildPackets Maintenance Member to download the following dll files. See the following URL:

https://wpdn.wildpackets.com/view_submission.php?id=30

- Copy the following dll files:
  - socket.dll file to the Plugins folder (Example: C:\ProgramFiles\WildPackets\AiroPeek\Plugins)
  - socketres.dll file to the PluginRes folder (Example:C:\ProgramFiles\WildPackets\AiroPeek\1033\PluginRes)

Configuring AiroPeek on the Remote Machine

To configure AiroPeek on the remote machine, follow these steps:

Step 1 Start the AiroPeek application and click **Options** on the Tools tab.

Step 2 Click **Analysis Module** in the Options page.

Step 3 Right-click inside the page and select **Disable All** option.

Step 4 Find the Cisco remote module column and enable it. Click **OK** to save the changes.

Step 5 Click **New capture** to bring up the capture option page.

Step 6 Choose the remote Cisco adapter and from the list of adapter modules.

Step 7 Expand it to locate the new remote adapter option. Double-click it to open a new page, enter a name in the text box provided and enter the controller management interface IP in the IP address column.

Step 8 Click **OK**. The new adapter is added to the remote Cisco adapter.

Step 9 Select the new adapter for remote airopeek capture using the access point.

Step 10 Click **start socket capture** in the capture page to start the remote capture process.

Step 11 From the controller CLI, bring up an access point, and set it to sniffer mode by entering the **config ap mode sniffer** *ap-name* command.

The access point reboots and comes up in sniffer mode.

Configuring an AP in Sniffer Mode Using the Web User Interface

To configure an AP in Sniffer mode using the web user interface, follow these steps:

Step 1 Choose **Configure > Access Points**, then click an item in the AP Name column to navigate to this page.

Step 2 In the General group box, set the AP mode to Sniffer using the drop-down list, and click **Apply**.

Step 3 Click a protocol (802.11a/802.11b/g) in the Protocol column in the Radio Interfaces group box. This opens the configuration page.

Step 4 Select the **Sniff** check box to bring up the Sniff parameters. Select the channel to be sniffed and enter the IP address of the server (The remote machine running AiroPeek).

Step 5 Click **Save** to save the changes.

Configuring 802.11 Parameters

Configuring General Parameters for an 802.11 Controller

This page enables you to edit country selection and timer information on a 802.11 controller. To access this page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11 > General**. The page opens and displays the following parameters:

- Country
  - Country—Countries and the protocols allowed.

    Note The maximum number of countries that you can select is 20.

  - Selected Countries—Displays countries currently selected.
- Timers
  - Authentication Response Timeout—Configures 802.11 authentication response timeout in seconds.

Setting Multiple Country Codes

To set multiple country support for a single controller(s) that is not part of a mobility group, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the controller for which you are adding countries.

Step 3 Choose **802.11 > General** from the left sidebar menu.

Step 4 Select the check box to choose which country you want to add. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that it complies with your country regulations.

Note Access points might not operate properly if they are not designed for use in your country of operation. For example, an access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Australia. Always be sure to purchase access points that match your country regulatory domain. For a complete list of country codes supported per product, see the following URL: http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html.

Step 5 Enter the time (in seconds) after which the authentication response times out.

Step 6 Click **Save**.

Configuring Aggressive Load Balancing

Enabling aggressive load balancing on the controller allows lightweight access points to load balance wireless clients across access points.

Note Clients are load balanced between access points on the same controller. Load balancing does not occur between access points on different controllers.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. This code indicates whether the access point can accept any more associations. If the access point is too busy, the client attempts to associate to a different access point in the area. The system determines if an access point is relatively more busy than its neighbor access points that are also accessible to the client.

For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it is allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

To configure aggressive load balancing, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the controller that you need to configure.

Step 3 Choose **802.11 > Load Balancing** from the left sidebar menu. The Load Balancing page appears (see Figure 8-11).

Figure 8-11 Load Balancing

Step 4 Enter a value between 1 and 20 for the client window size. The page size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

load-balancing page + client associations on AP with lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client page size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

Step 5 Enter a value between 0 and 10 for the max denial count. The denial count sets the maximum number of association denials during load balancing.

Step 6 Click **Save**.

Step 7 To enable or disable aggressive load balancing on specific WLANs, browse to the WLAN Configuration page, and click the **Advanced** tab. For instructions on using the WLAN Configuration page, see the "Configuring Controller WLANs" section on page 8-65.

Configuring Band Selection

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three non-overlapping channels. To combat these sources of interference and improve overall network performance, you can configure band selection on the controller.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels.

You can enable band selection globally on a controller, or you can enable or disable band selection for a particular WLAN, which is useful if you want to disable it for a select group of clients (such as time-sensitive voice clients).

Note Band-selection-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

Guidelines for Using Band Selection

Follow these guidelines when using band selection:

- Band selection can be used only with Cisco Aironet 1140 and 1250 series access points.
- Band selection operates only on access points that are connected to a controller. A FlexConnect access point without a controller connection does not perform band selection after a reboot.
- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.
- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.

Configuration Steps

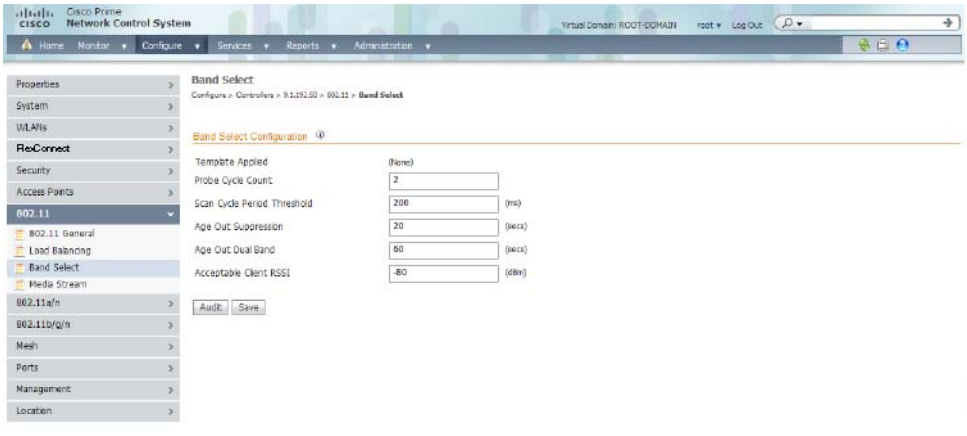
To configure band selection, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the controller that you need to configure.

Step 3 Choose **802.11 > Band Select** from the left sidebar menu. The Band Select page appears (see Figure 8-12).

Figure 8-12 Band Select



Step 4 Enter a value between 1 and 10 for the probe cycle count. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 5 Enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.

Step 6 Enter a value between 10 and 200 seconds for the age out suppression field. Age-out suppression sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 7 Enter a value between 10 and 300 seconds for the age out dual band field. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 8 Enter a value between –20 and –90 dBm for the acceptable client RSSI field. This field sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

Step 9 Click **Save**.

Step 10 To enable or disable band selection on specific WLANs, browse to the WLAN Configuration page and click the **Advanced** tab. For instructions on using the WLAN Configuration page, see the "Configuring Controller WLANs" section on page 8-65.

Configuring Preferred Call

The Preferred Call feature enables you to specify highest priority to SIP calls made to some specific numbers. The high priority is achieved by allocating bandwidth to such preferred SIP Calls even when there is no available voice bandwidth in the configured Voice Pool. This feature is supported only for those clients that use SIP based CAC for bandwidth allocation in WCS or WLC.

Note You can configure up to 6 numbers per controller.

To configure the preferred call support, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **802.11 > Preferred Call**. The following fields appear if there is an existing preferred call:

- Description—Description for the preferred call.
- Number Id—Indicates the unique identifier for the controller and denotes one of the six preferred call numbers assigned to the controller.
- Preferred Number—Indicates the preferred call number.

Step 4 From the Select a command drop-down list, choose **Add Number**.

Step 5 Select a template to apply to this controller.

Note You need to select a template to apply to the selected controller. To create a New Template for Preferred Call Numbers, see the "Configuring Preferred Call Templates" section on page 10-91.

Step 6 Click **Apply**.

Note To delete a preferred call, select the check box for the applicable preferred call number and choose **Delete** from the Select a command drop-down list. Click **Go** and then click **OK** to confirm the deletion.

Configuring 802.11 Media Parameters

To configure the media parameters for 802.11, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the applicable IP address.

Step 3 From the left sidebar menu, choose **802.11 > Media Stream**.

Step 4 In the Media Stream Configuration section, configure the following parameters

- Media Stream Name
- Multicast Destination Start IP—Start IP address of the media stream to be multicast
- Multicast Destination End IP—End IP address of the media stream to be multicast
- Maximum Expected Bandwidth—Maximum bandwidth that a media stream can use

Step 5 In the Resource Reservation Control (RRC) Parameters group box, configure the following parameters:

- Average Packet Size—Average packet size that a media stream can use.
- RRC Periodical Update—Resource Reservation Control calculations that are updated periodically; if disabled, RRC calculations are done only once when a client joins a media stream.
- RRC Priority—Priority of RRC with the highest at 1 and the lowest at 8.
- Traffic Profile Violation—Appears if the stream is dropped or put in the best effort queue if the stream violates the QoS video profile.

- Policy—Appears if the media stream is admitted or denied.

Step 6 Click **Save**.

Configuring RF Profiles (802.11)

The RF Profiles page enables you to create or modify RF profiles that get associated to AP Groups.

To configure a RF Profile for a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click **RF Profiles** or choose either **802.11 > RF Profiles** from the left sidebar menu. The RF Profiles page appears. This page lists the existing RF Profile templates.

Step 3 If you want to add a RF profile, choose **Add RF Profile** from the Select a command drop-down list.

Step 4 Click **Go**. The New Controller Template page appears.

Step 5 Configure the following information:

- General
  - Template Name—User-defined name for the template.
  - Profile Name—User-defined name for the current profile.
  - Description—Description of the template.
  - Radio Type—The radio type of the access point. This is a drop-down list from which you can choose an RF profile for APs with 802.11a or 802.11b radios.
- TCP (Transmit Power Control)
  - Minimum Power Level Assignment (-10 to 30 dBm)—Indicates the minimum power assigned. The range is -10 to 30 dB, and the default value is 30 dB.
  - Maximum Power Level Assignment (-10 to 30 dBm)—Indicates the maximum power assigned. The range is -10 to 30 dB, and the default value is 30 dB.
  - Power Threshold v1(-80 to -50 dBm)—Indicates the transmitted power threshold.
  - Power Threshold v2(-80 to -50 dBm)—Indicates the transmitted power threshold.
- Data Rates—Use the Data Rates drop-down lists to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:
  - 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps.
  - 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.

  For each data rate, choose one of these options:
  - Mandatory—Clients must support this data rate to associate to an access point on the controller.
  - Supported—Any associated clients that support this data rate might communicate with the access point using that rate. However, the clients are not required to be able to use this rate to associate.
  - Disabled—The clients specify the data rates used for communication.

Step 6 Click **Save**.

Configuring 802.11a/n Parameters

This section contains the following topics:

Configuring 802.11a/n General Parameters

To view 802.11a/n parameters for a specific controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n Parameters** to view the following parameters:

- General
  - 802.11a/n Network Status—Select the check box to enable.
  - Beacon Period—The amount of time between beacons. The valid range is from 100 to 600 milliseconds.
  - DTIM Period—The number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count field is 0.
  - Fragmentation Threshold (in bytes)—The size at which packets are fragmented. Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
  - Template Applied
- 802.11a/n Band Status
  - Low, Medium, and High Bands (read-only).
- 802.11a/n Power Status
  - Dynamic Assessment—Automatic, On Demand, or Disabled.
  - Current Tx Level—Range includes: 1 (maximum power allowed per country code setting), 2 (50% power), 3 (25% power), 4 (6.25 to 12.5% power), and 5 (0.195 to 6.25% power).

Note The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

  - Control Interval—In seconds (read-only).
  - Dynamic Treatment Power Control—Select the check box to enable.
- 802.11a/n Channel Status
  - Assignment Mode—Automatic, On Demand, or Disabled.
  - Update Interval—In seconds.
  - Avoid Foreign AP Interference—Enable to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels.
  - Avoid Cisco AP load—Enable to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points.
  - Avoid non 802.11 Noise—Enable to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Disable this field to have RRM ignore this interference.
  - Signal Strength Contribution—Not configurable.
  - Avoid Persistent Non-WiFi interface
- Data Rates
  - Ranges between 6 Mbps and 54 Mbps—Supported, Mandatory, or Disabled.
- Noise/Interference/Rogue Monitoring Channels.
  - Channel List—All Channels, Country Channels, DCA Channels.

Note Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation from a set of managed devices connected to the controller.

- CCX Location Measurement—When enabled, it enhances the location accuracy of clients.
  - Mode—Select the check box to enable.
  - Interval—In seconds.

Note The CCX Location Measurement Interval can be changed only when measurement mode is enabled.

Command Buttons

- Save—Save the changes made.
- Audit—Compare the NCS values with those used on the controller.

Configuring 802.11a/n RRM Thresholds

To configure a 802.11a/n RRM threshold controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM Thresholds**.

Step 4 Make any necessary changes to Coverage Thresholds, Load Thresholds, Other Thresholds, and Noise/Interference/Rogue Monitoring Channels.

Note When the Coverage Thresholds Min SNR Level (dB) field is adjusted, the value of the Signal Strength (dB) automatically reflects this change. The Signal Strength (dB) field provides information regarding what the target range of coverage thresholds is when adjusting the SNR value.

Step 5 Click **Save**.

Configuring 802.11a/n RRM Intervals

To configure 802.11a/n or 802.11b/g/n RRM intervals for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM Intervals** or **802.11b/g/n > RRM Intervals**.

Note The default for the following four RRM interval parameters is 300 seconds.

Step 4 Enter at which interval you want strength measurements taken for each access point.

Step 5 Enter at which interval you want noise and interference measurements taken for each access point.

Step 6 Enter at which interval you want load measurements taken for each access point.

Step 7 Enter at which interval you want coverage measurements taken for each access point.

Step 8 Click **Save**.

Configuring 802.11a/n RRM Transmit Power Control

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of the access point according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

Transmit Power Control version 2 (TPCv2) attempts to reduce the co-channel interference from Cisco AP networks. The former version of TPC is designed to provide strong signal coverage with a tendency to use larger Tx Power, and as a result customers were suffering from overheating in densely deployed networks.

To configure 802.11a/n or 802.11b/g/n RRM TPC, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n-RRM > TPC**.

Step 4 Configure the following TPC parameters:

- Template Applied—The name of the template applied to this controller.
- Template Version—Indicates the TPC version.

  The TPCv2 option is applicable only for those controllers running 7.2.x release or later.
- Dynamic Assignment—At the Dynamic Assignment drop-down list, choose one of three modes:
  - Automatic - The transmit power is periodically updated for all access points that permit this operation.
  - On Demand - Transmit power is updated when the Assign Now button is selected.
  - Disabled - No dynamic transmit power assignments occur, and values are set to their global default.
- Maximum Power Assignment—Indicates the maximum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Minimum Power Assignment—Indicates the minimum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Dynamic Tx Power Control—Determine if you want to enable Dynamic Tx Power Control.
- Transmitted Power Threshold—Enter a transmitted power threshold between -50 and -80.
- Control Interval—In seconds (read-only).

Step 5 Click **Save**.

Configuring 802.11a/n RRM Dynamic Channel Allocation

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.

Note Choosing a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments.

To configure 802.11 a/n RRM DCA channels for an individual controller, follow these steps:

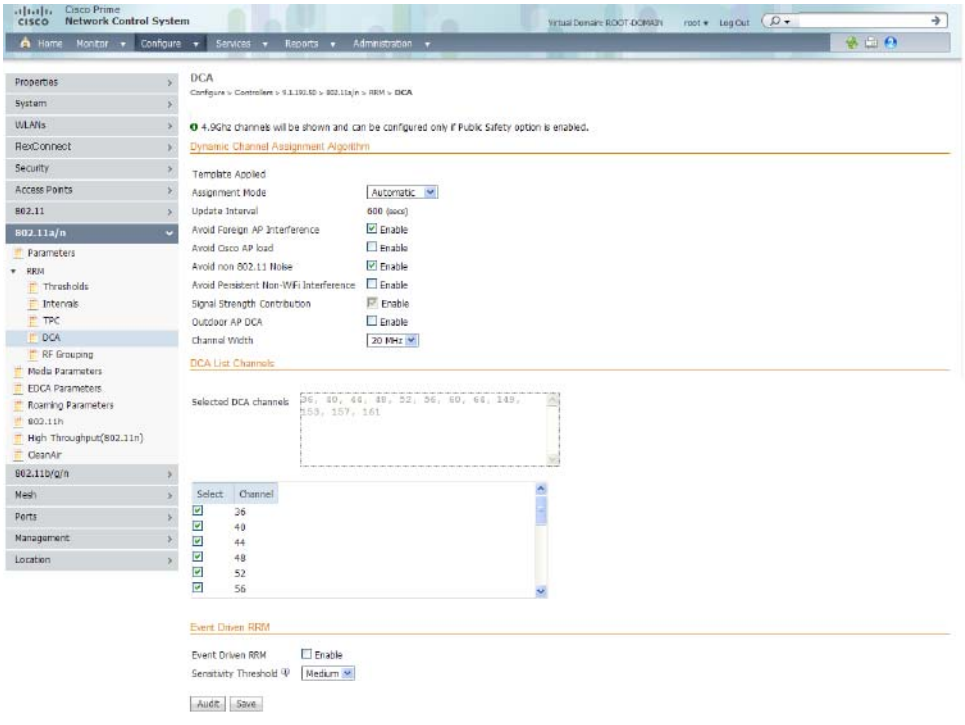
Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM DCA**. The 802.11a/n RRM DCA page appears (see Figure 8-13).

Note You can also configure the channel width on the access point page by choosing **Configure > Access Points**, and clicking the **802.11a/n** link in the Radio column. The Current RF Channel Assignment. is provided, and you can choose a Global assignment method or choose Custom to specify a channel.

Figure 8-13 802.11a/n RRM DCA Page



Step 4 From the Channel Width drop-down list, choose **20 MHz** or **40 MHz**. Prior to software release 5.1, 40-MHz channels were only statically configurable. Only radios with 20-MHz channels were supported by DCA. With 40 MHz, radios can achieve higher instantaneous data rates; however, larger bandwidths reduce the number of non-overlapping channels so certain deployments could have reduced overall network throughput.

Note Be cautious about deploying a mix of 20-MHz and 40-MHz devices. The 40-MHz devices have slightly different channel access rules which might negatively impact the 20-MHz devices.

Note To view the channel width for the radio of an access point, go to **Monitor > Access Points >** *name* **> Interfaces** tab. You can also view the channel width and antenna selections by choosing **Configure > Access Points** and clicking the desired radio in the Radio column.

Step 5 Select the check boxes for the appropriate DCA channels. The selected channels are listed in the Selected DCA channels list.

Step 6 Enable or disable event-driven Radio Resource Management (RRM) using the following parameters. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference.

- Event Driven RRM—Enable or Disable spectrum event-driven RRM. By default, Event Driven RRM is enabled.
- Sensitivity Threshold—If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Step 7 Click **Save**.

Configuring 802.11a/n RRM Radio Grouping

To configure 802.11a/n or 802.11b/g/n RRM Radio Grouping for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM > RF Grouping**.

Step 4 Choose a grouping mode from the drop-down list. The following parameters appear:

- Automatic—Allows you to activate the automatic RRM Grouping Algorithm. This is the default mode.
- Off—Allows you to deactivate the automatic grouping.
- Leader—Allows you to assign members to the group.

Step 5 Choose a group update interval (secs) from the drop-down list. When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. The grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 600 seconds.

Step 6 In the Group Members group box, click **Add >**. The selected controller moves from the Available Controllers to the RF Group Members list.

Note The RF Group Members group box appears only when the grouping mode is set to Leader.

Note The maximum number of controllers that can be added to a RF Group is 20.

Step 7 Click **Save**.

Configuring 802.11a/n Media Parameters

To configure the media parameters for 802.11a/n, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > Media Parameters**.

Step 4 On the **Voice** tab, configure the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.

  For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, Call Admission Control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.

- CAC Method—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.

  Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

  In load-based CAC, the access point periodically measures and updates the utilization of the RF channel, channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents over-subscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

- Maximum Bandwidth Allowed—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.

- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.

- Expedited Bandwidth—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.

  You must have an expedited bandwidth that is CCXv5 compliant so that a TSPEC request is given higher priority.

- SIP CAC—Select the check box to enable SIP CAC.

  SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.

- SIP Codec—Specify the codec name you want to use on this radio. The available options are G.711, G.729, and User Defined.
- SIP Call Bandwidth—Specify the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.
- SIP Sample Interval—Specify the sample interval in milliseconds that the codec must operate in.
- Max Voice Calls per Radio—Specify the maximum number of voice calls that can be made per Radio.
- Max Roaming Reserved Calls per Radio—Specify the maximum number roaming calls that can be reserved per Radio.

Note The Max Voice Calls per Radio and Max Roaming Reserved Calls per Radio options are available only if the CAC Method is specified as Static and SIP CAC is enabled.

- Metric Collection—Select the check box to enable metric collection.

  Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Step 5 On the **Video** tab, configure the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.
- Maximum Bandwidth Allowed—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
- Unicast Video Redirect—Select the **Unicast Video Redirect** check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
- Client Minimum Phy Rate—Choose the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
- Multicast Direct Enable—Select the **Multicast Direct Enable** check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
- Maximum Number of Streams per Radio—Specify the maximum number of streams per Radio to be allowed.
- Maximum Number of Streams per Client—Specify the maximum number of streams per Client to be allowed.

- Best Effort QOS Admission—Select the **Best Effort QOS Admission** check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used.

Note If disabled and maximum video bandwidth has been used, then any new client request is rejected.

Step 6 On the **General** tab, configure the following field:

- Maximum Media Bandwidth (0 to 85%)—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Step 7 Click **Save**.

Note SIPs are available only on the following controllers: 4400, 5500. Also, SIPs are available only for the following access points: 1240, 1130, and 11n.

Command Buttons

- Save—Save the changes made.
- Audit—Compare the NCS values with those used on the controller.

Configuring 802.11a/n EDCA Parameters

The EDCA parameters (EDCA profile and Streaming MAC Enable settings) for 802.11a/n and 802.11b/g/n can be configured either by individual controller or through a controller template to improve voice QoS support.

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > EDCA Parameters** or **802.11b/g/n > EDCA Parameters**.

Step 4 Choose the EDCA Profile from the drop-down list.

Note Profiles include Wi-Fi Multimedia (WMM), Spectralink Voice Priority (SVP), Voice Optimized, and Voice & Video Optimized. WMM is the default EDCA profile.

Note You must shut down radio interface before configuring EDCA Parameters.

Step 5 Select the **Enable Streaming MAC** check box to enable this feature.

Note Only enable Streaming MAC if all clients on the network are WMM compliant.

Configuring 802.11a/n Roaming Parameters

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > Roaming Parameters**.

Step 4 From the Mode drop-down list, choose **Default values** or **Custom values**.

- Default values—The default values (read-only) are automatically displayed in the text boxes.
- Custom values—Activates the text boxes to enable editing of the roaming parameters.

Step 5 In the Minimum RSSI text box, enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point.

- Range: -80 to -90 dBm
- Default: -85 dBm

Note If the client average received signal power dips below this threshold, reliable communication is typically impossible; clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

Step 6 In the Hysteresis text box, enter a value to indicate how strong the signal strength of a neighboring access point must for the client to roam to it.

This field is intended to reduce the amount of "ping ponging" between access points if the client is physically located on or near the border between two access points.

- Range: 2 to 4 dB
- Default: 3 dB

Step 7 In the Adaptive Scan Threshold text box, enter the RSSI value, from a client associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time.

This field provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.

- Range: -70 to -77 dB
- Default: -72 dB

Step 8 In the Transition Time text box, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client associated access point is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

- Range: 1 to 10 seconds
- Default: 5 seconds

Step 9 Click **Save**.

Configuring 802.11a/n 802.11h Parameters

To configure 802.11h parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > 802.11h** or **802.11b/g/n > 802.11h**.

Step 4 Select the **power constraint** check box to enable TPC.

Step 5 Select the **channel announcement** check box to enable channel announcement. Channel announcement is a method in which the access point announces when it is switching to a new channel and the new channel number.

Step 6 Click **Save**.

Configuring 802.11a/n High Throughput (802.11n) Parameters

To configure 802.11a/n or 802.11b/g/n high throughput parameters, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > High Throughput** or **802.11b/g/n > High Throughput**.

Step 4 Select the **802.11n Network Status Enabled** check box to enable high throughput.

Step 5 In the MCS (Data Rate) Settings, choose which level of data rate you want supported. MCS is modulation coding schemes which are similar to 802.11a data rate. As a default, 20 MHz and short guarded interval is used.

Note When you select the Supported check box, the chosen numbers appear in the Selected MCS Indexes page.

Step 6 Click **Save**.

Configuring 802.11a/n CleanAir Parameters

To configure 802.11a/n CleanAir parameters, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > CleanAir** to view the following information.

- CleanAir—Select the check box to enable CleanAir functionality on the 802.11 a/n network, or unselect to disable CleanAir functionality. The default value is selected.
- Reporting Configuration—Use the parameters in this section to configure the interferer devices you want to include for your reports.
  - Report—Select the **report interferers** check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.
  - Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect text box and any that do not need to be detected appear in the Interferers to Ignore text box. Use the > and < buttons to move interference sources between these two text boxes. By default, all interference sources are detected.
  - Select the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables designating information about interference types and propagating this information to the neighboring access points. Persistent interferers are present at the a location and interfere with the WLAN operations even if they are not detectable at all times.
- Alarm Configuration—This section enables you to configure triggering of air quality alarms.
  - Air Quality Alarm—Select the **Air Quality Alarm** check box to enable the triggering of air quality alarms, or unselect the box to disable this feature. The default value is selected.
  - Air Quality Alarm Threshold—If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.
  - Air Quality Unclassified category Alarm—Select the **Air Quality Unclassified category Alarm** check box to enable the alarms to be generated for unclassified interference category. CleanAir can detect and monitor unclassified interferences. Unclassified interference are interference that are detected but do not correspond to any of the known interference types.

    The Unclassified category alarm is generated when the unclassified severity goes above the configured threshold value for unclassified severity or when the air quality index goes below the configured threshold value for Air Quality Index.
  - Air Quality Unclassified Category Severity Threshold—If you selected the Air Quality Unclassified category Alarm check box, enter a value between 1 and 99 (inclusive) in the Air Quality Unclassified Severity Threshold text box to specify the threshold at which you want the unclassified category alarm to be triggered. The default is 20.
  - Interferers For Security Alarm—Select the **Interferers For Security Alarm** check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is selected.

  - Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms text box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms text box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.
- Event Driven RRM—To trigger spectrum event-driven Radio Resource Management (RRM) to run when a CleanAir-enabled access point detects a significant level of interference, follow these steps:
  - Event Driven RRM—Displays the current status of spectrum event-driven RRM.
  - Sensitivity Threshold—If Event Driven RRM is enabled, this text box displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Command Buttons

- Save—Save the changes made.
- Audit—Compare the NCS values with those used on the controller.

Configuring 802.11b/g/n Parameters

This section contains the following topics:

Configuring 802.11b/g/n General Parameters

To view 802.11b/g/n parameters for a specific controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11b/g/n Parameters** to view the following parameters:

- General
  - 802.11b/g Network Status—Select the check box to enable.
  - 802.11g Support—Select the check box to enable.
  - Beacon Period—In milliseconds.
  - DTIM Period—The number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count field is 0.
  - Fragmentation Threshold—In bytes.
  - Short Preamble—Select the check box to enable.
  - Template Applied.
- 802.11a/n Power Status
  - Dynamic Assessment—Automatic, On Demand, or Disabled.
  - Current Tx Level.
  - Control Interval—In seconds (Read-only).
  - Dynamic Treatment Power Control—Select the check box to enable.
- 802.11a/n Channel Status
  - Assignment Mode—Automatic, On Demand, or Disabled.
  - Update Interval—In seconds.
  - Avoid Foreign AP Interference—Select the check box to enable.
  - Avoid Cisco AP load—Select the check box to enable.
  - Avoid non 802.11 Noise—Select the check box to enable.
  - Signal Strength Contribution—Select the check box to enable.
- Data Rates
  - Ranges between 1 Mbps and 54 Mbps—Supported, Mandatory, or Disabled.
- Noise/Interference/Rogue Monitoring Channels
  - Channel List—All Channels, Country Channels, DCA Channels.
- CCX Location Measurement
  - Mode—Select the check box to enable.
  - Interval—In seconds.

Note The CCX Location Measurement Interval can be changed only when measurement mode is enabled.

Command Buttons

- Save—Save the changes made.
- Audit—Compare the NCS values with those used on the controller.

Configuring 802.11b/g/n RRM Thresholds

To configure a 802.11b/g/n RRM threshold controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11b/g/n > RRM Thresholds**.

Step 4 Make any necessary changes to Coverage Thresholds, Load Thresholds, Other Thresholds, and Noise/Interference/Rogue Monitoring Channels.

Note When the Coverage Thresholds Min SNR Level (dB) field is adjusted, the value of the Signal Strength (dB) automatically reflects this change. The Signal Strength (dB) field provides information regarding what the target range of coverage thresholds is when adjusting the SNR value.

Step 5 Click **Save**.

Configuring 802.11b/g/n RRM Intervals

To configure 802.11a/n or 802.11b/g/n RRM intervals for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM Intervals** or **802.11b/g/n > RRM Intervals**.

Note The default for the following four RRM interval parameters is 300 seconds.

Step 4 Enter at which interval you want strength measurements taken for each access point.

Step 5 Enter at which interval you want noise and interference measurements taken for each access point.

Step 6 Enter at which interval you want load measurements taken for each access point.

Step 7 Enter at which interval you want coverage measurements taken for each access point.

Step 8 Click **Save**.

Configuring 802.11b/g/n RRM Transmit Power Control

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of an access point according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

To configure 802.11b/g/n RRM TPC, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11b/g/n-RRM > TPC**.

Step 4 Configure the following TPC parameters:

- Template Applied—The name of the template applied to this controller.
- Dynamic Assignment—At the Dynamic Assignment drop-down list, choose one of three modes:
  - **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
  - **On Demand**—Transmit power is updated when the Assign Now button is selected.
  - **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.
- Maximum Power Assignment—Indicates the maximum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Minimum Power Assignment—Indicates the minimum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Dynamic Tx Power Control—Determine if you want to enable Dynamic Tx Power Control.
- Transmitted Power Threshold—Enter a transmitted power threshold between -50 and -80.
- Control Interval—In seconds (read-only).

Step 5 Click **Save**.

Configuring 802.11b/g/n RRM DCA

To configure 802.11a/n or 802.11b/g/n RRM DCA channels for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11b/g/n-RRM > DCA**.

Step 4 Select the check box(es) for the applicable DCA channel(s). The selected channels are listed in the Selected DCA channels text box.

Step 5 Enable or disable event-driven Radio Resource Management (RRM). Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference, follow these steps:

- Event Driven RRM—Enable or Disable spectrum event-driven RRM. By default, Event Driven RRM is enabled.
- Sensitivity Threshold—If Event Driven RRM is enabled, this text box displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity

Step 6 Click **Save**.

Configuring 802.11b/g/n RRM Radio Grouping

To configure 802.11a/n or 802.11b/g/n RRM Radio Grouping for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11b/g/n > RRM > RF Grouping**.

Step 4 Choose a grouping mode from the drop-down list. The following parameters appear:

- **Automatic**—Allows you to activate the automatic RRM Grouping Algorithm. This is the default mode.
- **Off**—Allows you to deactivate the automatic grouping.
- **Leader**—Allows you to assign members to the group.

Step 5 Choose a group update interval (secs) from the drop-down list. When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. The default value is 600 seconds.

Step 6 In the Group Members group box, click **Add >**. The selected controller moves from the Available Controllers to the RF Group Members list.

Note The RF Group Members group box appears only when the grouping mode is set to Leader.

Note The maximum number of controllers that can be added to a RF Group is 20.

Step 7 Click **Save**.

Configuring 802.11b/g/n Media Parameters

To configure the media parameters for 802.11b/g/n, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the applicable IP address.

Step 3 From the left sidebar menu, choose **802.11b/g/n > Media Parameters**.

Step 4 In the Voice tab, configure the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.

  For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, Call Admission Control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.

- CAC Method—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.

  Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

  In load-based CAC, the access point periodically measures and updates the utilization of the RF channel, channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents over-subscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

- Maximum Bandwidth Allowed—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.

- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.

- Expedited Bandwidth—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.

  You must have an expedited bandwidth that is CCXv5 compliant so that a TSPEC request is given higher priority.

- SIP CAC—Select the check box to enable SIP CAC.

  SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.

- SIP Codec—Specify the codec name you want to use on this radio. The available options are G.711, G.729, and User Defined.

- SIP Call Bandwidth—Specify the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.

- SIP Sample Interval—Specify the sample interval in milliseconds that the codec must operate in.

- Max Voice Calls per Radio—Indicates the maximum number of voice calls that can be made per Radio.

Note You cannot set the value of Max Voice Calls per Radio. This is automatically calculated based on the selected CAC method, Max BW allowed, and Roaming Bandwidth.

- Max Roaming Reserved Calls per Radio—Indicates the maximum number roaming calls that can be reserved per Radio.

Note The Max Voice Calls per Radio and Max Roaming Reserved Calls per Radio options are available only if the CAC Method is specified as Static and SIP CAC is enabled.

- Metric Collection—Select the check box to enable metric collection.

  Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Step 5 In the **Video** tab, configure the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.
- Maximum Bandwidth—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
- Unicast Video Redirect—Select the **Unicast Video Redirect** check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
- Client Minimum Phy Rate—Specify the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
- Multicast Direct Enable—Select the **Multicast Direct Enable** check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
- Maximum Number of Streams per Radio—Specify the maximum number of streams per Radio to be allowed.
- Maximum Number of Streams per Client—Specify the maximum number of streams per Client to be allowed.
- Best Effort QOS Admission—Select the **Best Effort QOS Admission** check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used.

Note If disabled and maximum video bandwidth has been used, then any new client request is rejected.

Step 6 On the **General** tab, configure the following field:

- Maximum Media Bandwidth (0 to 85%)—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Step 7 Click **Save**.

Note SIPs are available only on the following controllers: 4400, 5500. Also, SIPs are available only for the following access points: 1240, 1130, and 11n.

Command Buttons

- Save—Save the changes made.
- Audit—Compare the NCS values with those used on the controller.

Configuring 802.11b/g/n EDCA Parameters

The EDCA parameters (EDCA profile and Streaming MAC Enable settings) for 802.11a/n and 802.11b/g/n can be configured either by individual controller or through a controller template to improve voice QoS support.

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > EDCA Parameters** or **802.11b/g/n > EDCA Parameters**.

Step 4 Choose the EDCA Profile from the drop-down list.

Note Profiles include Wi-Fi Multimedia (WMM), Spectralink Voice Priority (SVP), Voice Optimized, and Voice & Video Optimized. WMM is the default EDCA profile.

Note You must shut down radio interface before configuring EDCA Parameters.

Step 5 Select the **Enable Streaming MAC** check box to enable this feature.

Note Only enable Streaming MAC if all clients on the network are WMM compliant.

Configuring 802.11b/g/n Roaming Parameters

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > Roaming Parameters** or **802.11b/g/n > Roaming Parameters**.

Step 4 From the Mode drop-down list, choose **Default values** or **Custom values**.

- Default values—The default values (read-only) are automatically displayed in the text boxes.
- Custom values—Activates the text boxes to enable editing of the roaming parameters.

Step 5 In the Minimum RSSI text box, enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point.

- Range: -80 to -90 dBm
- Default: -85 dBm

Note If the client average received signal power dips below this threshold, reliable communication is typically impossible; clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

Step 6 In the Hysteresis text box, enter a value to indicate how strong the signal strength of a neighboring access point must be in order for the client to roam to it.

This field is intended to reduce the amount of "ping ponging" between access points if the client is physically located on or near the border between two access points.

- Range: 2 to 4 dB
- Default: 3 dB

Step 7 In the Adaptive Scan Threshold text box, enter the RSSI value, from a client associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time.

This field provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.

- Range: -70 to -77 dB
- Default: -72 dB

Step 8 In the Transition Time text box, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client associated access point is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

- Range: 1 to 10 seconds
- Default: 5 seconds

Step 9 Click **Save**.

Configuring 802.11b/g/n High Throughput (802.11n) Parameters

To configure 802.11a/n or 802.11b/g/n high throughput parameters, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > High Throughput** or **802.11b/g/n > High Throughput**.

Step 4 Select the **802.11n Network Status Enabled** check box to enable high throughput.

Step 5 In the MCS (Data Rate) Settings, choose which level of data rate you want supported. MCS is modulation coding schemes which are similar to 802.11a data rate. As a default, 20 MHz and short guarded interval is used.

Note When you select the Supported check box, the chosen numbers appear in the Selected MCS Indexes page.

Step 6 Click **Save**.

Configuring 802.11b/g/n CleanAir Parameters

To configure 802.11b/g/n CleanAir parameters, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11b/g/n > CleanAir** to view the following information.

- CleanAir—Select the check box to enable CleanAir functionality on the 802.11b/g/n network, or unselect to prevent the controller from detecting spectrum interference. The default value is selected.
- Reporting Configuration—Use the parameters in this section to configure the interferer devices you want to include for your reports.
  - Report—Select the **report interferers** check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.
  - Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect text box and any that do not need to be detected appear in the Interferers to Ignore text box. Use the > and < buttons to move interference sources between these two text boxes. By default, all interference sources are detected.
  - Select the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables designating information about interference types and propagating this information to the neighboring access points. Persistent interferers are present at a location and interfere with the WLAN operations even if they are not detectable at all times.
- Alarm Configuration—This group box enables you to configure triggering of air quality alarms.
  - Air Quality Alarm—Select the **Air Quality Alarm** check box to enable the triggering of air quality alarms, or unselect the text box to disable this feature. The default value is selected.
  - Air Quality Alarm Threshold—If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

  - Air Quality Unclassified category Alarm—Select **Air Quality Unclassified category Alarm** check box to enable the alarms to be generated for unclassified interference category. Cisco CleanAir can detect and monitor unclassified interferences. Unclassified interference are interference that are detected but do not correspond to any of the known interference types.

    The Unclassified category alarm is generated when the unclassified severity goes above the configured threshold value for unclassified severity or when the air quality index goes below the configured threshold value for Air Quality Index.
  - Air Quality Unclassified Category Severity Threshold—If you selected the Air Quality Unclassified category Alarm check box, enter a value between 1 and 99 (inclusive) in the Air Quality Unclassified Severity Threshold text box to specify the threshold at which you want the unclassified category alarm to be triggered. The default is 20.
  - Interferers For Security Alarm—Select the **Interferers For Security Alarm** check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is selected.
  - Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms text box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms text box. Use the **>** and **<** buttons to move interference sources between these two text boxes. By default, all interference sources trigger interferer alarms.

- Event Driven RRM—To trigger spectrum event-driven Radio Resource Management (RRM) to run when a CleanAir-enabled access point detects a significant level of interference, use the following parameters:
  - Event Driven RRM—Displays the current status of spectrum event-driven RRM.
  - Sensitivity Threshold—If Event Driven RRM is enabled, this text box displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Allocation (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Command Buttons

- Save—Save the changes made.
- Audit—Compare the NCS values with those used on the controller.

Configuring Mesh Parameters

To configure Mesh parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Mesh > Mesh Settings**.

Step 4 View or edit the following mesh parameters:

- RootAP to MeshAP Range (150 - 13200 ft)—By default, this value is 12,000 feet. You can enter a value between 150 and 132,000 feet. Enter the optimum distance (in feet) that should exist between the root access point and the mesh access point. This global field applies to all access points when they join the controller and all existing access points in the network.
- Client Access on Backhaul Link—Enabling this feature lets mesh access points associate with 802.11a wireless clients over the 802.11a backhaul. This client association is in addition to the existing communication on the 802.11a backhaul between the root and mesh access points. This feature is only applicable to access points with two radios. For more information, see the "Client Access on 1524SB Dual Backhaul" section on page 8-147.

Note Changing Backhaul Client Access reboots all mesh access points.

- Mesh DCA Channels—Enable or disable. This option is disabled by default. Enable this option to enable backhaul channel deselection on the controller using the DCA channel list. Any change to the channels in the Controller DCA list is pushed to the associated access points. This option is only applicable for 1524SB mesh access points. For more information on this feature, see the "Backhaul Channel Deselection Using the NCS" section on page 8-148.
- Background Scanning—Select the **Background Scanning** check box to enable background scanning or unselect it to disable the feature. The default value is disabled. Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents.
- Security Mode—Choose **EAP** (Extensible Authentication Protocol) or **PSK** (Pre-Shared Key) from the Security Mode drop-down list.

Note Changing Security reboots all mesh access points.

Step 5 Click **Save**.

Client Access on 1524SB Dual Backhaul

The 1524 Serial Backhaul (SB) access point consists of three radio slots. Radio in slot-0 operate in 2.4 GHz frequency band which is used for client access. Radios in slot-1 and slot-2 operate in 5.8 GHz band and are primarily used for backhaul. However, with the Universal Client Access feature, client access is also allowed over slot-1 and slot-2 radios.

The two 802.11a backhaul radios use the same MAC address. There might be instances where the same WLAN maps to the same BSSID in more than one slot.

By default, client access is disabled over both of the backhaul radios.

The following guidelines should be followed for enabling or disabling a radio slot:

- You can enable client access on slot-1 even if client access on slot-2 is disabled.
- You can enable client access on slot-2 only when client access on slot-1 is enabled.
- If you disable client access on slot-1 the client access on slot-2 is automatically disabled.
- All the Mesh Access Points reboot whenever the client access is enabled or disabled.

You can configure client access over backhaul radio from either one of the following:

- The Controller command-line interface (CLI)

- The Controller Graphical User Interface (GUI)
- The NCS GUI. For more information, see the "Configuring Client Access Using the NCS - GUI" section on page 8-148.

Note The procedure for configuring client access using the CLI and GUI is documented in the *Controller Configuration Guide*.

Configuring Client Access Using the NCS - GUI

To configure client access on the two backhaul radios, follow these steps:

Step 1 Choose **Configure > Controllers > Controller IP > Mesh > Mesh Settings**.

Step 2 Select the **Client Access on Backhaul Link** check box.

Step 3 Select the **Extended Backhaul Client Access** check box if you want to enable extended backhaul client access.

Step 4 Click **Save**.

A warning message is displayed:

```
Enabling client access on both backhaul slots will use same BSSIDs on both the slots.
Changing Backhaul Client Access will reboot all Mesh APs.
```

Step 5 Click **OK**.

The Universal Client access is configured on both the radios.

Backhaul Channel Deselection Using the NCS

To configure backhaul channel deselection, follow these steps:

Step 1 You must first configure the Mesh DCA channels flag on the controllers. See the "Configuring Mesh DCA Channel Flag on Controllers Using the NCS" section on page 8-148 for more information.

Step 2 Then change the channel list using config groups. See the "Changing the Channel List Using Config Groups" section on page 8-149 for more information.

This section contains the following topics:

Configuring Mesh DCA Channel Flag on Controllers Using the NCS

You can configure the Mesh DCA Channel flag to push each channel change on one or more controllers to all the associated 1524SB access points. To configure this feature, follow these steps:

Step 1 Choose **Configure > Controllers >** *ip address of controller* **> Mesh > Mesh Settings** to configure this flag for a specific controller.

Or

Configure > Controller Template Launch Pad > Mesh > Mesh Settings to configure this flag for a list of controllers.

The Mesh Settings page appears.

Step 2 From the general options select the **Mesh DCA Channels** option to enable channel selection. This option is unselected by default.

Now the channel changes in the controllers are pushed to the associated 1524SB access points.

Changing the Channel List Using Config Groups

You can use controller config groups to configure backhaul channel deselection. You can create a config group and add the required controllers into the group and use the Country/DCA tab to select or deselect channels for the controllers in that group.

To configure backhaul channel deselection using config groups, follow these steps:

Step 1 Choose **Configure > Controller Config Groups**.

Step 2 Select a config group to view its config group details.

Step 3 From the Config Group detail page, click the **Country/DCA** tab.

Step 4 Select or unselect the channels for the config group.

Note You can also configure backhaul channel deselection from controllers. For more information, see the Controller Online Help or *Controller User Guide*.

Configuring Port Parameters

To configure Port parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Ports > Port Settings**.

Step 4 Click the applicable Port Number to open the Port Settings Details page. The following parameters display:

- General Parameters:
  - Port Number—Read-only.
  - Admin Status—Choose Enabled or Disabled from the drop-down list.
  - Physical Mode—Choose Auto Negotiate or Full Duplex 1 Gbps.
  - STP Mode—Choose 802.1D, Fast, or Off.
  - Mirror Mode—Choose Enabled or Disabled.

  - Link Traps—Choose Enabled or Disabled.
  - Power Over Ethernet
  - Multicast Application Mode—Select Enabled or Disabled.
- Spanning Tree Protocol Parameters:
  - Priority—The numerical priority number of the ideal switch.
  - Path Cost—A value (typically based on hop count, media bandwidth, or other measures) assigned by a network administrator and used to determine the most favorable through an internetwork environment (the lower the cost, the better the path).

Step 5 Choose **Save** or **Audit** for General or Spanning Tree Protocol settings.

Configuring Controllers Management Parameters

This section contains the following topics:

Configuring Trap Receivers

This section contains the following topics:

Configuring Trap Receivers for an Individual Controller

To configure trap receivers for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Trap Receivers**.

Step 4 The following parameters are displayed for current trap receivers:

- Template Name—User-defined name of this template.
- IP Address—The IP address of the server.
- Admin Status—Status must be enabled for the SNMP traps to be sent to the receiver.

Step 5 Click a receiver Name to access its details.

Step 6 Select the **Admin Status** check box to enable the trap receiver. Unselect the check box to disable the trap receiver.

Step 7 Click **Save**.

Adding a New Receiver

To add a new receiver, follow these steps:

Step 1 From the Select a command drop-down list, choose **Add Receiver**.

Step 2 Click **Go**.

Step 3 From the Select a template to apply to this controller drop-down list, choose the applicable template to apply to this controller.

Note To create a new template for Trap Receivers, use the **click here** link to access the applicable template creation page.

Step 4 Click **Apply**.

Configuring Trap Control Parameters

To configure trap control parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Trap Control**.

The applied template is identified (if applicable). See the "Configuring Trap Control Templates" section on page 10-124 for more information.

The following traps can be enabled for this controller:

- Miscellaneous Traps
  - SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated.

    Note When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

  - Link (Port) Up/Down—Link changes status from up or down.
  - Multiple Users—Two users login with the same login ID.
  - Spanning Tree—Spanning Tree traps. See the STP specifications for descriptions of individual parameters.

  - Rogue AP—Whenever a rogue access point is detected this trap is sent with its MAC address; When a rogue access point that was detected earlier and it no longer exists this trap is sent.
  - Config Save—Notification sent when the controller configuration is modified.
- Client Related Traps
  - 802.11 Association—The associate notification is sent when the client sends an association frame.
  - 802.11 Disassociation—The disassociate notification is sent when the client sends a disassociation frame.
  - 802.11 Deauthentication—The deauthenticate notification is sent when the client sends a deauthentication frame.
  - 802.11 Failed Authentication—The authenticate failure notification is sent when the client sends an authentication frame with a status code other than 'successful'.
  - 802.11 Failed Association—The associate failure notification is sent when the client sends an association frame with a status code other than 'successful'.
  - Excluded—The associate failure notification is sent when a client is excluded.
- Cisco AP Traps
  - AP Register—Notification sent when an access point associates or disassociates with the controller.
  - AP Interface Up/Down—Notification sent when access point interface (802.11a or 802.11b/g) status goes up or down.
- Auto RF Profile Traps
  - Load Profile—Notification sent when Load Profile state changes between PASS and FAIL.
  - Noise Profile—Notification sent when Noise Profile state changes between PASS and FAIL.
  - Interference Profile—Notification sent when Interference Profile state changes between PASS and FAIL.
  - Coverage Profile—Notification sent when Coverage Profile state changes between PASS and FAIL.
- Auto RF Update Traps
  - Channel Update—Notification sent when access point dynamic channel algorithm is updated.
  - Tx Power Update—Notification sent when access point dynamic transmit power algorithm is updated.
- AAA Traps
  - User Auth Failure—This trap is to inform that a client RADIUS Authentication failure has occurred.
  - RADIUS Server No Response—This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.
- IP Security Traps
  - ESP Authentication Failure—IPsec packets with invalid hashes were found in an inbound ESP SA.
  - ESP Replay Failure—IPsec packets with invalid sequence numbers were found in an inbound ESP SA.

  - Invalid SPI—A packet with an unknown SPI was detected from the specified peer with the specified SPI using the specified protocol.
  - IKE Negotiation Failure—An attempt to negotiate a phase 1 IKE SA failed. The notification counts are also sent as part of the trap, along with the current value of the total negotiation error counters.
  - IKE Suite Failure—An attempt to negotiate a phase 2 SA suite for the specified selector failed. The current total failure counts are passed as well as the notification type counts for the notify involved in the failure.
  - Invalid Cookie—ISAKMP packets with invalid cookies were detected from the specified source, intended for the specified destination. The initiator and responder cookies are also sent with the trap.
- 802.11 Security Traps
  - WEP Decrypt Error—Notification sent when the controller detects a WEP decrypting error.
- WPS Traps
  - Rogue Auto Containment—Notification sent when a rogue access point is auto-contained.

Step 4 After selecting the applicable parameters, click **Save**.

Configuring Telnet SSH Parameters

To configure Telnet SSH (Secure Shell) parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Telnet SSH**.

The applied template is identified (if applicable). See the "Configuring Telnet SSH Templates" section on page 10-126 for more information.

The following parameters can be configured:

- Session Timeout—Indicates the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. Might be specified as a number from 0 to 160. The factory default is 5.
- Maximum Sessions—From the drop-down list, choose a value from 0 to 5. This object indicates the number of simultaneous Telnet sessions allowed.

  Note New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service port.

- Allow New Telnet Sessions—Indicates that new Telnet sessions are not allowed on the DS Port when set to no. The factory default value is no.

  Note New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service port.

- Allow New SSH Sessions—Indicates that new Secure Shell Telnet sessions are not allowed when set to no. The factory default value is yes.

Step 4 After configuring the applicable parameters, click **Save**.

Configuring a Syslog for an Individual Controller

To enable a Syslog for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Syslog**.

The applied template is identified (if applicable). See the "Configuring Legacy Syslog Templates" section on page 10-127 for more information.

- **Syslog Enabled**—Select the check box to enable the syslog.

Step 4 Click **Save**.

Configuring Multiple Syslog Servers

For Release 5.0.148.0 controllers or later, you can configure multiple (up to three) syslog servers on the WLAN controller. With each message logged, the controller sends a copy of the message to each configured syslog host, provided the message has severity greater than or equal to the configured syslog filter severity level.

To enable syslogs for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Multiple Syslog**.

The applied template is identified:

Syslog Server Address—Indicates the server address of the applicable syslog.

Step 4 Click **Save**.

Configuring WEB Admin

This section provides instructions for enabling the distribution system port as a web port (using HTTP) or as a secure web port (using HTTPS). You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Sockets Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You also have the option of downloading an externally generated certificate.

To enable WEB admin parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Web Admin**.

The following parameters can be configured:

- Web Mode—Choose **Enable** or **Disable** from the drop-down list. When enabled, users can access the controller GUI using *http:ip-address*. The default is Disabled.

  Note Web mode is not a secure connection.

- Secure Web Mode—Choose **Enable** or **Disable** from the drop-down list. When enabled, users can access the controller GUI using *https://ip-address*. The default is Enabled.

  Note Secure web mode is a secure connection.

- Certificate Type
- Download Web Admin Certificate—Click to access the Download Web Admin Certificate to Controller page. See the "Downloading Web Auth or Web Admin Certificate to the Controller" section on page 8-155 for additional information.

  Note The controller must be rebooted for the new Web Admin certificate to take effect.

Command Buttons

- Save
- Audit
- Regenerate Cert

Downloading Web Auth or Web Admin Certificate to the Controller

To download a Web Auth or Web Admin Certificate to the controller, follow these steps:

Step 1 Click the **Download Web Admin Certificate** or **Download Web Auth Certificate** link.

Step 2 In the File is located on field, specify Local machine or TFTP server.

Note If the certificate is located on the TFTP server, enter the server filename. If it is located on the local machine, click **Browse** and enter the local filename.

Step 3 Enter the TFTP server name in the **Server Name** text box. The default is the NCS server.

Step 4 Enter the server IP address.

Step 5 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 6 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 7 In the Local File Name text box, enter the directory path of the certificate.

Step 8 In the Server File Name text box, enter the name of the certificate.

Step 9 Enter the password in the Password text box.

Step 10 Click **OK**.

Configuring Local Management Users

This page lists the names and access privileges of the local management users.

To access the Local Management Users page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Local Management Users**.

Step 4 Click a username.

- User Name (read-only)—Name of the user.
- Access Level (read-only)—Read Write or Read Only.

Configuring Authentication Priority

In this page, you can control the order in which authentication servers are used to authenticate a controller management users.

To access the Authentication Priority page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Authentication Priority**.

Step 4 The local database is searched first. Choose either RADIUS or TACACS+ for the next search. If authentication using the local database fails, the controller uses the next type of server.

Step 5 Click **Save**.

Command Buttons

- Save—Save the changes made to the management user authentication order and return to the previous page.
- Audit—Compare the NCS values with those used on the controller.

Configuring Location Configurations

In the Location Configuration page, you can configuration location parameters such as expiration times, notification interval, and other advanced configuration options.

You can set the following general and advanced parameters on the location template:

- General parameters—Enable RFID tag collection, set the location path loss for calibrating or normal (non-calibrating) clients, measurement notification for clients, tags, and rogue access points, set the RSSI expiry timeout value for clients, tags, and rogue access points.
- Advanced parameters–Set the RFID tag data timeout value and enable the location path loss configuration for calibrating client multi-band.

To configure location configurations for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Location Configuration > Location Configuration**.

The Location Configuration page displays two tabs: General and Advanced.

Step 4 Add or modify the General parameters:

- RFID Tag Data Collection—Select the check box to enable the collection of data on tags.

  Before the location server can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command **config rfid status enable** on the controllers.

- Location Path Loss Configuration
  - Calibrating Client—Select the **Enabled** check box to enable calibration for the client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrate clients. Packets are transmitted on all channels. All access points gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic.

    Note To use all radios (802.11a/b/g/n) available, you must enable multiband in the Advanced page.

  - Normal Client—Select the **Enabled** check box to have a non-calibrating client. No S36 requests are transmitted to the client.

    Note S36 and S60 are client drivers compatible with specific Cisco Compatible Extensions. S36 is compatible with CCXv2 or later. S60 is compatible with CCXv4 or later. For details, see the following URL: http://www.cisco.com/en/US/products/ps9806/products_qanda_item09186a0080af9513.shtml

- Measurement Notification Interval (in secs)
  - Tags, Clients, and Rogue APs/Clients—Allows you to set the NMSP measurement notification interval for clients, tags, and rogues. Specify how many seconds should elapse before notification of the found element (tags, clients, and rogue access points/clients).

Setting this value on the controller generates an out-of-sync notification which you can view in the Synchronize Servers page. When different measurement intervals exist between a controller and the mobility services engine, the largest interval setting of the two is adopted by the mobility services engine.

Once this controller is synchronized with the mobility services engine, the new value is set on the mobility services engine.

Note Synchronization to the mobility services engine is required if changes are made to measurement notification interval.

- RSS Expiry Timeout (in secs)
  - For Clients—Enter the number of seconds after which RSSI measurements for normal (non-calibrating) clients should be discarded.
  - For Calibrating Clients—Enter the number of seconds after which RSSI measurements for calibrating clients should be discarded.
  - For Tags—Enter the number of seconds after which RSSI measurements for tags should be discarded.
  - For Rogue APs—Enter the number of seconds after which RSSI measurements for rogue access points should be discarded.

Step 5 Add or modify the Advanced parameters:

- RFID Tag Data Timeout (in secs)—Enter a value (in seconds) to set the RFID tag data timeout setting.
- Location Path Loss Configuration
  - Calibrating Client Multiband—Select the **Enabled** check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enable in the general page.

Note To use all radios (802.11a/b/g/n) available, you must enable multiband.

Step 6 Click **Save**.

Command Buttons

- Save—Save the changes made to the management user authentication order and return to the previous page.
- Audit—Compare the NCS values with those used on the controller.uld be discarded.

Configuring IPv6

This section contains the following topics:

Configuring Neighbor Binding Timers

You can configure IPv6 Router Neighbor Binding Timers parameters such as Down Lifetime, Reachable Lifetime, State Lifetime, and corresponding intervals.

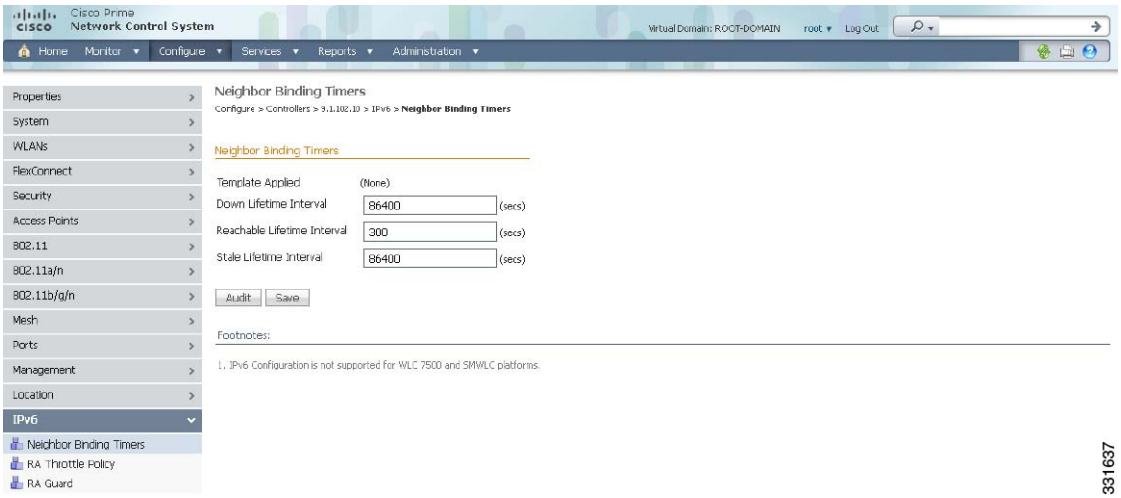
To configure Neighbor Binding Timers, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 Choose **IPv6 > Neighbor Binding Timers** from the left sidebar menu. The IPv6 > Neighbor Binding Timers page appears (see Figure 8-14).

Figure 8-14 Neighbor Binding Timers Page



Step 4 If you want to enable the Down Lifetime timer, select the **Enable** check box. If you have selected this check box, specify the Down Lifetime Interval value. This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.

Step 5 If you want to enable the Reachable Lifetime timer, select the **Enable** check box. If you have selected this check box, specify the Reachable Lifetime Interval value. This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.

Step 6 If you want to enable the Stale Lifetime timer, select the **Enable** check box. If you have selected this check box, specify the Stale Lifetime Interval value. This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.

Step 7 Click **Save**.

Configuring RA Throttle Policy

The RA Throttle Policy allows you to limit the amount of multicast Router Advertisements (RA) circulating on the wireless network. You can configure IPv6 Router Advertisement parameters such as RA Throttle Policy, Throttle Period and other options.

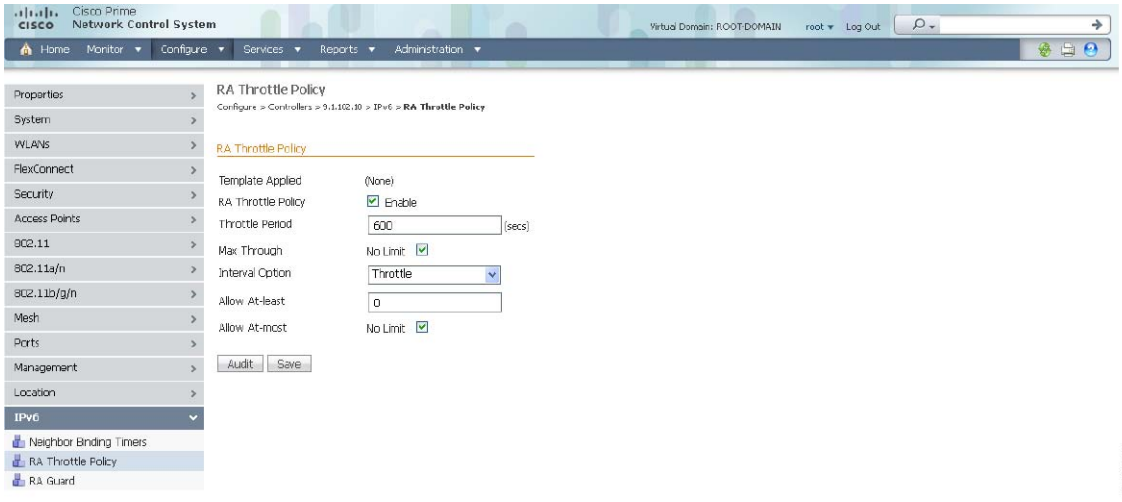
To configure RA Throttle Policy, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 Choose **IPv6 > RA Throttle Policy** from the left sidebar menu. The IPv6 > RA Throttle Policy page appears (see Figure 8-15).

Figure 8-15 RA Throttle Policy Page



Step 4 If you want to enable the RA Throttle Policy, select the **Enable** check box and configure the following parameters:

- Throttle Period—Duration of the throttle period in seconds. The range is 10 to 86,400 seconds.
- Max Through—The number of RA that passes through over a period or over an unlimited period.
- Interval Option—Indicates the behavior in case of RA with an interval option.
  - Ignore
  - Passthrough
  - Throttle
- Allow At-least—Indicates the minimum number of RA not throttled per router.
- Allow At-most—Indicates the maximum or unlimited number of RA not throttled per router.

Step 5 Click **Save**.

Configuring RA Guard

RA Guard is a Unified Wireless solution to drop RA from wireless clients. It is configured globally, and by default it is enabled. You can configure IPv6 Router Advertisement parameters.

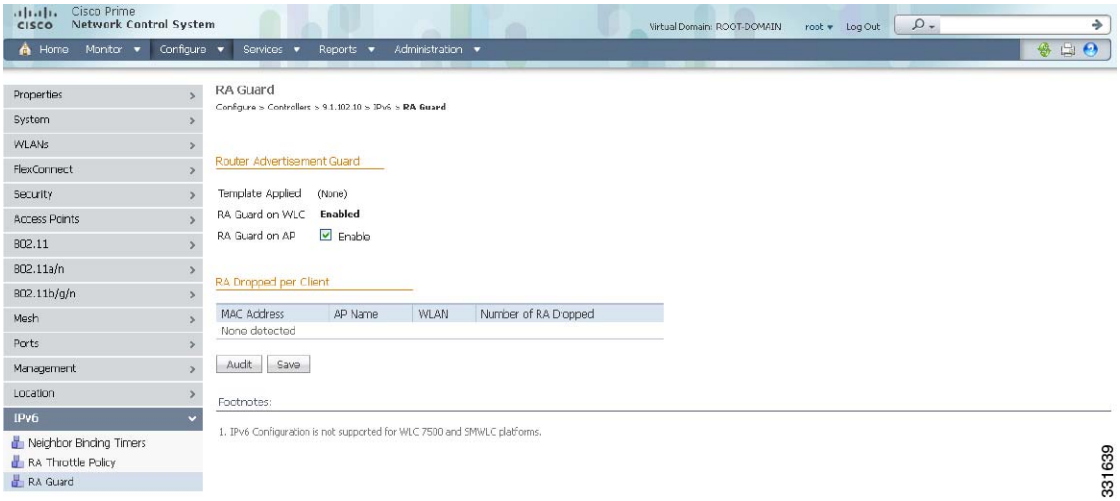
To configure RA Guard, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 Choose **IPv6 > RA Guard** from the left sidebar menu. The IPv6 > RA Guard page appears (see Figure 8-16).

Figure 8-16 RA Guard Page



Step 4 If you want to enable the Router Advertisement Guard, select the **Enable** check box.

Step 5 Click **Save**.

Configuring Access Points

This section describes how to configure access points in the NCS database. This section contains the following topics:

Setting AP Failover Priority

When a controller fails, the backup controller configured for the access point suddenly receives a number of discovery and join requests. This might cause the controller to reach a saturation point and reject some of the access points.

By assigning priority to an access point, you have some control over which access points are rejected. In a failover situation when the backup controller is saturated, the higher priority access points are allowed to join the backup controller by disjoining the lower priority access points.

To configure priority settings for access points, you must first enable the AP Priority feature. To enable the AP Priority feature, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > General**.

Step 4 From the AP Failover Priority drop-down list, choose **Enable**.

To configure the priority of an access point, see the "Configuring Access Point Details" section on page 8-174.

Configuring Global Credentials for Access Points

Cisco autonomous access points are shipped from the factory with *Cisco* as the default enable password. This password allows users to log into the non-privileged mode and execute show and debug commands, posing a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the console port of an access point.

In the NCS and controller software releases prior to 5.0, you can set the access point enable password only for access points that are currently connected to the controller. In the NCS and controller software release 5.0, you can set a global username, password, and enable password that all access points inherit as they join a controller. This includes all access points that are currently joined to the controller and any that join in the future. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis and assign a unique username, password, and enable password. See the "Configuring AP Configuration Templates" section on page 10-137 to see where the global password is displayed and how it can be overridden on a per-access point basis.

Also in controller software release 5.0, after an access point joins the controller, the access point enables console port security, and you are prompted for your username and password whenever you log into the console port of an access point. When you log in, you are in non-privileged mode, and you must enter the enable password to use the privileged mode.

Note These controller software release 5.0 features are supported on all access points that have been converted to lightweight mode, except the 1100 series. VxWorks access points are not supported.

The global credentials that you configure on the controller are retained across controller and access point reboots. They are overwritten only if the access point joins a new controller that is configured with a global username and password. If the new controller is not configured with global credentials, the access point retains the global username and password configured for the first controller.

Note You need to keep careful track of the credentials used by the access points. Otherwise, you might not be able to log into the console port of an access point. If necessary, you can clear the access point configuration to return the access point username and password to the default setting.

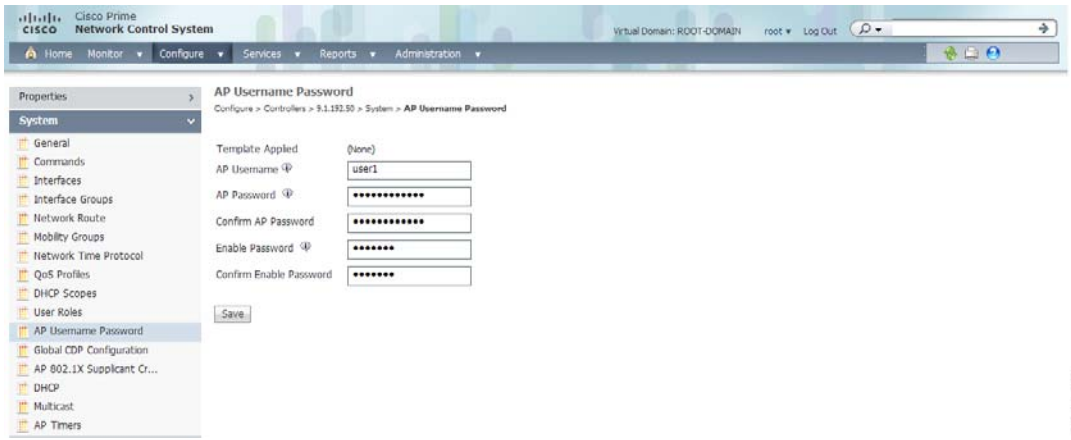
To establish a global username and password, follow these steps:

Step 1 Choose **Configure > Controllers** or **Configure > Access Points**.

Step 2 Choose an IP address of a controller with software release 5.0 or later or choose an access point associated with software release 5.0 or later.

Step 3 Choose **System > AP Username Password** from the left sidebar menu. The AP Username Password page appears (see Figure 8-17).

Figure 8-17 AP Username Password Page



Step 4 In the AP Username text box, enter the username that is to be inherited by all access points that join the controller.

Step 5 In the AP Password text box, enter the password that is to be inherited by all access points that join the controller. Reenter the password in the Confirm AP Password text box.

Step 6 For Cisco autonomous access points, you must also enter and confirm an enable password. In the AP Enable Password text box, enter the enable password that is to be inherited by all access points that join the controller. Reenter the password in the Confirm Enable Password text box.

Step 7 Click **Save**.

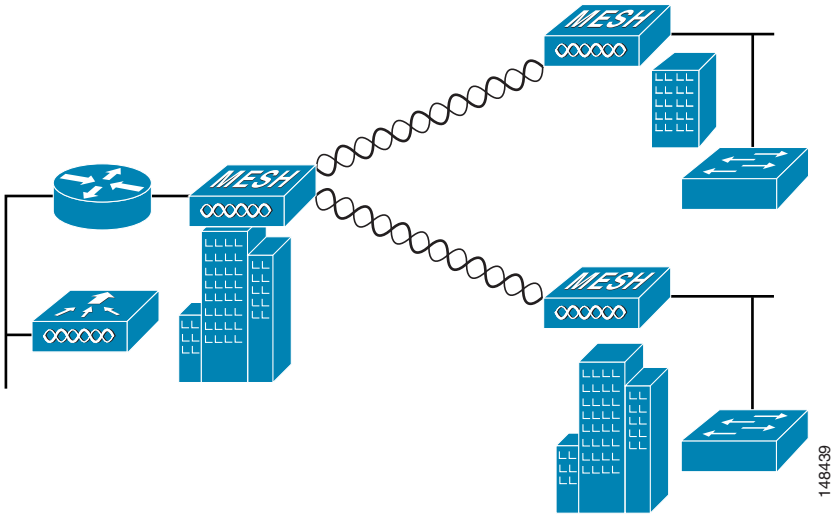
Configuring Ethernet Bridging and Ethernet VLAN Tagging

Ethernet bridging is used in two mesh network scenarios:

1. Point-to-point and point-to-multipoint bridging between MAPs (untagged packets). A typical trunking application might be bridging traffic between buildings within a campus (see Figure 8-18).

Note You do not need to configure VLAN tagging to use Ethernet bridging for point-to-point and point-to-multipoint bridging deployments.

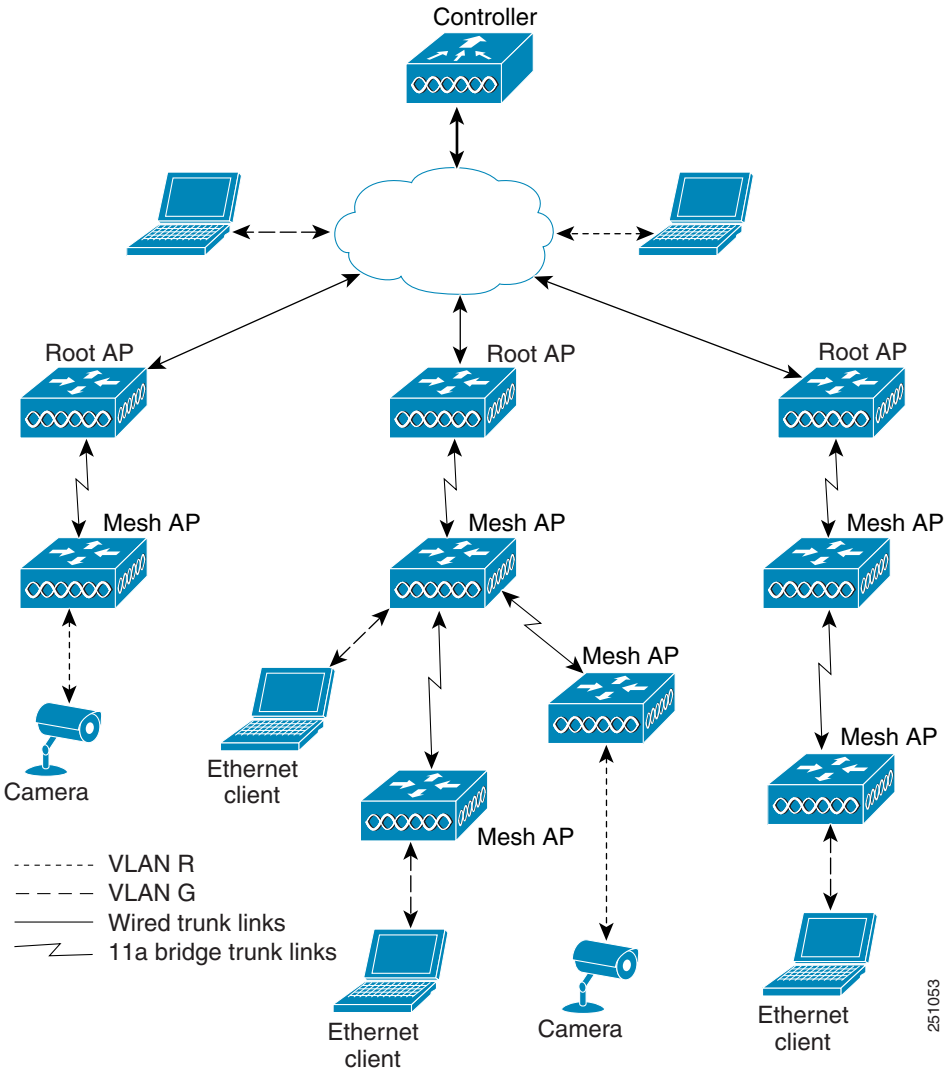
Figure 8-18 Point-to-Multipoint Bridging



2. Ethernet VLAN tagging allows specific application traffic to be segmented within a wireless mesh network and then forwarded (bridged) to a wired LAN (access mode) or bridged to another wireless mesh network (trunk mode).

A typical public safety access application using Ethernet VLAN tagging is placement of video surveillance cameras at various outdoor locations within a city. Each of these video cameras has a wired connection to a MAP. The video of all these cameras is then streamed across the wireless backhaul to a central command station on a wired network (see Figure 8-19).

Figure 8-19 Ethernet VLAN Tagging



Ethernet VLAN Tagging Guidelines

- For security reasons, the Ethernet port on a mesh access point (RAP and MAP) is disabled by default. It is enabled by configuring Ethernet Bridging on the mesh access point port.
- You must enable Ethernet bridging on all the access points in the mesh network to allow Ethernet VLAN Tagging to operate.
- You must set VLAN Mode as non-VLAN transparent (global mesh field). See the "Configuring Ethernet Bridging and Ethernet VLAN Tagging" section on page 8-164.
  - VLAN transparent is enabled by default. To set as non-VLAN transparent, you must unselect the VLAN transparent option in the Global Mesh Parameters page.
- VLAN configuration on a mesh access point is only applied if all the uplink mesh access points are able to support that VLAN.

  - If uplink access points are not able to support the VLAN, then the configuration is stored rather than applied.
- VLAN tagging can only be configured on Ethernet interfaces.
  - On 152x mesh access points, use three of the four ports as *secondary Ethernet interfaces*: *port 0-PoE in, port 1-PoE out, and port 3- fiber.* You cannot configure *Port 2 - cable* as a secondary Ethernet interface.
  - In Ethernet VLAN tagging, *port 0-PoE in* on the RAP connects the trunk port of the switch of the wired network. *Port 1-PoE out* on the MAP connects external devices such as video cameras.
- Backhaul interfaces (802.11a radios) act as *primary Ethernet interfaces*. Backhauls function as trunks in the network and carry all VLAN traffic between the wireless and wired network. You are not required to configure the primary Ethernet interface.
- You must configure the switch port in the wired network that is attached to the RAP (*port 0–PoE in*) to accept tagged packets on its trunk port. The RAP forwards all tagged packets received from the mesh network to the wired network.
- Configuration to support VLAN tagging on the 802.11a backhaul Ethernet interface is not required within the mesh network.
  - This includes the RAP uplink Ethernet port. The required configuration happens automatically using a registration mechanism.
  - Any configuration changes to an 802.11a Ethernet link acting as a backhaul are ignored, and a warning results. When the Ethernet link no longer functions as a backhaul, the modified configuration is applied.
- You cannot configure VLANs on port-02-cable modem port of a 152x access point. Configure VLANs on ports 0 (PoE-in), 1 (PoE-out), and 3 (fiber).
- If bridging between two MAPs, enter the distance (mesh range) between the two access points that are bridging. (Not applicable to applications in which you are forwarding traffic connected to the MAP to the RAP, access mode.)
- Each sector supports up to 16 VLANs; therefore, the cumulative number of VLANs supported by the children of a RAP (MAPs) cannot exceed 16.
- Ethernet ports on access points function as *normal*, *access,* or *trunk* ports in an Ethernet tagging deployment.
  - Normal mode—In this mode, the Ethernet interface is VLAN-transparent by default and does not accept or send any tagged packets. Tagged frames from clients are dropped. Untagged frames are forwarded to the native VLAN on the RAP trunk port.
  - Access mode—In this mode only untagged packets are accepted. You must tag all packets with a user-configured VLAN called access-VLAN. For this mode to take effect, the global VLAN mode should be non-VLAN transparent.

    Use this option for applications in which information is collected from devices connected to the MAP such as cameras or PCs and then forwarded to the RAP. The RAP then applies tags and forwards traffic to a switch on the wired network.
  - Trunk mode—This mode requires the user to configure a native VLAN and an allowed VLAN list (no defaults). In this mode, both tagged and untagged packets are accepted. You can accept untagged packets and tag them with the user-specified native VLAN. You can accept tagged packets if they are tagged with a VLAN in the allowed VLAN list. For this mode to take effect, the global VLAN mode should be non-VLAN transparent.

Use this option for bridging applications such as forwarding traffic between two MAPs resident on separate buildings within a campus.

- The switch port connected to the RAP must be a trunk.
  - The trunk port on the switch and the RAP trunk port must match.
- A configured VLAN on a MAP Ethernet port cannot function as a Management VLAN.
- The RAP must always connect to the native VLAN (ID 1) on a switch.
  - The primary Ethernet interface of the RAP is by default the native VLAN of 1.

Enabling Ethernet Bridging and VLAN Tagging

To enable Ethernet Bridging and VLAN tagging on a RAP or MAP, follow these steps:

Step 1 Choose **Configure > Access Points**.

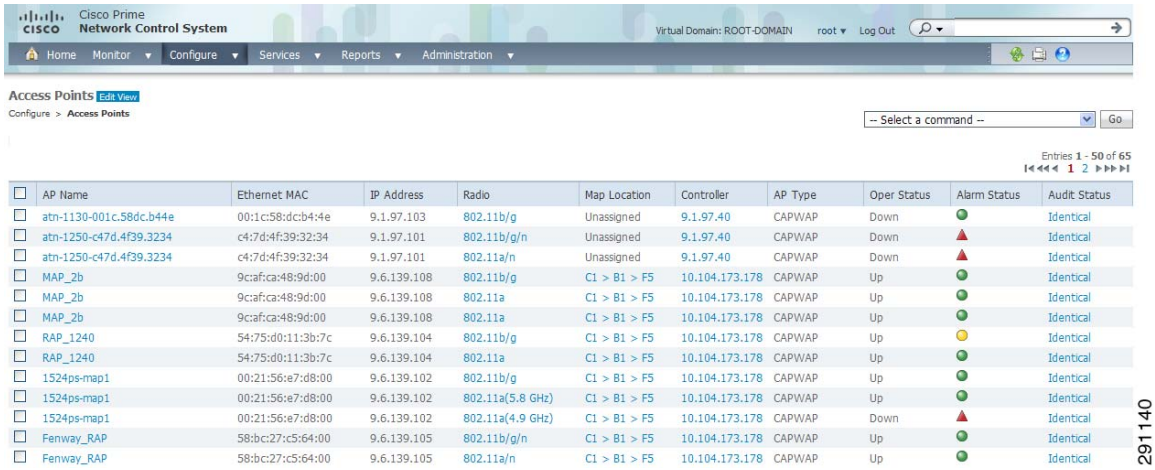
Step 2 Click the name of the mesh access point for which you want to enable Ethernet bridging. A configuration page for the access point appears.

Step 3 In the Bridging Information group box, choose the appropriate backhaul rate from the Data Rate drop-down list. The default value is 24 Mbps for the 802.11a backhaul interface.

Step 4 In the Bridging Information section, choose **Enable** from the Ethernet Bridging drop-down list.

Step 5 Click the appropriate Ethernet interface link (such as FastEthernet or gigabitEthernet1). (See Figure 8-20.)

Figure 8-20 Configure > Access Points > AP Name Page



Step 6 In the Ethernet interface page, perform one of the following:

Note The configuration options vary for each of the VLAN modes (normal, access, and trunk).

a. If you are configuring a MAP and RAP normal ports and chose FastEthernet0, choose **Normal** from the VLAN Mode drop-down list.

In this mode, the Ethernet interface is VLAN-transparent by default and does not accept or send any tagged packets. Tagged frames from clients are dropped. Untagged frames are forwarded to the native VLAN on the RAP trunk port.

b. If you are configuring a MAP access port and chose **gigabitEthernet1** (port 1-PoE out):

1. Choose **Access** from the VLAN Mode drop-down list.
2. Enter a VLAN ID. The VLAN ID can be any value between 1 and 4095.
3. Click **Save**.

Note VLAN ID 1 is not reserved as the default VLAN.

Note A maximum of 16 VLANs in total are supported across all of the subordinate MAPs of a RAP.

c. If you are configuring a RAP or MAP trunk port and chose **gigabitEthernet0** (or **FastEthernet0**) (port 0-PoE in),

1. Choose **trunk** from the VLAN Mode drop-down list.
2. Enter a native VLAN ID for *incoming* traffic. The native VLAN ID can be any value between 1 and 4095. Do not assign any value assigned to a user-VLAN (access).
3. Enter a trunk VLAN ID for *outgoing* traffic, and click **Add**.

   The added trunk appears in the summary column of allowed VLAN IDs.

   If forwarding *untagged* packets, do not change the default trunk VLAN ID value of zero (such as MAP-to-MAP bridging, campus environment).

   If forwarding *tagged* packets, enter a VLAN ID (1 to 4095) that is not already assigned (such as RAP to switch on wired network).

Note To remove a VLAN from the list, click **Delete**.

4. Click **Save**.

Note At least one mesh access point must be set to RootAP in the mesh network.

Autonomous to Lightweight Migration Support

The autonomous to lightweight migration support feature provides a common application (the NCS) from which you can perform basic monitoring of autonomous access points along with current lightweight access points. The following autonomous access points are supported:

- Cisco Aironet 1130 Access Point
- Cisco Aironet 1200 Access Point
- Cisco Aironet 1240 Access Point

- Cisco Aironet 1310 Bridge
- Cisco Aironet 1410 Bridge

You might also choose to convert autonomous access points to lightweight. Once an access point is converted to lightweight, the previous status or configuration of the access point is not retained.

From the NCS, the following functions are available when managing autonomous access points:

- Adding Autonomous Access Points to the NCS, page 8-169
- Viewing Autonomous Access Points in the NCS, page 8-173
- Adding and viewing autonomous access points from the Monitor > Maps page (see the "Monitoring Maps" section on page 4-1 for more information)
- Monitoring associated alarms
- Performing an autonomous access point background task
  - Checks the status of autonomous access points managed by the NCS.
  - Generates a critical alarm when an unreachable autonomous access point is detected.
- Running reports on autonomous access points
  - See Reports > Inventory Reports and Reports > Client Reports > Client Count for more information
- Supporting Autonomous Access Points in Work Group Bridge (WGB) mode, page 8-174
- Migrating an Autonomous Access Point to a Lightweight Access Point, page 10-139Migrating an Autonomous Access Point to a Lightweight Access Point, page 10-149Migrating an Autonomous Access Point to a Lightweight Access Point, page 10-149Migrating an Autonomous Access Point to a Lightweight Access Point, page 10-149Migrating an Autonomous Access Point to a Lightweight Access Point, page 10-149Migrating an Autonomous Access Point to a Lightweight Access Point, page 10-149

Adding Autonomous Access Points to the NCS

From the NCS, the following methods are available for adding autonomous access points:

- Adding Autonomous Access Points by Device Information, page 8-169 (IP addresses and credentials).
- Adding Autonomous Access Points by CSV File, page 8-170.
- Removing Autonomous Access Points, page 8-173

Adding Autonomous Access Points by Device Information

Autonomous access points can be added to the NCS by device information using comma-separated IP addresses and credentials.

To add autonomous access points using device information, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 From the Select a command drop-down list, choose **Add Autonomous APs**.

Step 3 Click **Go**.

Step 4 Choose **Device Info** from the Add Format Type drop-down list.

Step 5 Enter comma-separated IP addresses of autonomous access points.

Step 6 Enter the SNMP Parameters parameters:

- Version—Choose from v1, v2, or v3.
- Retries—Indicates the number of controller discovery attempts.
- Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The valid range is 2 to 90 seconds. The default is 10 seconds.
- Community—Public or Private.

Step 7 Enter the Telnet/SSH Parameters:

Note Default values are used if the Telnet/SSH parameters are left blank.

- Protocol—Select the protocol you want to use (either Telenet or SSH).
- User Name—Enter the username. (The default username is admin.)

Note The Telnet/SSH username must have sufficient privileges to execute commands in CLI templates.

- Password/Confirm Password—Enter and confirm the password. (Default password is admin.)
- Enable Password/Confirm Password—Enter and confirm an enable password.
- Telnet Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The default is 60 seconds.

Note Cisco autonomous access points are shipped from the factory with *Cisco* as the default enable password. This password allows users to log into the non-privileged mode and execute show and debug commands, posing a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the console port of an access point.

Step 8 Click **Add**.

Note After the AP is added and its inventory collection is completed, it appears in the Access Point list page (Configure > Access Points). If it is not found in the Access Points list, choose **Configure > Unknown Device** page to check the status. For details, see the "Configuring Unknown Devices" section on page 8-209.

Note Autonomous access points are not counted towards the total device count for your license.

Adding Autonomous Access Points by CSV File

Autonomous access points can be added to the NCS using a CSV file exported from WLSE.

To add autonomous access points using a CSV file, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 From the Select a command drop-down list, choose **Add Autonomous APs**.

Step 3 Click **Go**.

Step 4 Choose **File** from the Add Format Type drop-down list.

Step 5 Enter or browse to the applicable CSV file.

The sample CSV files for V2 devices are as follows:

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name,
snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password,
snmp_retries, snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v2,public,,,,,3,4
209.165.201.0,255.255.255.0,v2,public,,,,,3,4,Cisco,Cisco,2,10
```

Note The SNMP, telnet, or SSH credentials are mandatory.

The sample CSV files for V3 devices are as follows:

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type,
snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v3,default,HMAC-MD5,default,None,,3,4
209.165.201.0,255.255.255.224,v3,default1,HMAC-MD5,default1,DES,default1,3,4,Cisco,Cisco,2
,10
```

The CSV files can contain the following fields:

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- telnet_username
- telnet_password
- enable_password
- telnet_retries
- telnet_timeout

Step 6 Click **OK**.

Bulk Update of Autonomous Access Points

You can update multiple autonomous access points credentials by importing a CSV file.

To update autonomous access point(s) information in a bulk, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 From the Select a command drop-down list, choose **Bulk Update APs**. The Bulk Update Autonomous Access Points page appears.

Step 4 Click **Choose File** to select a CSV file, and then find the location of the CSV file you want to import.

Step 5 Click **Update and Sync**.

Sample CSV File for the Bulk Update of Autonomous Access Points

The sample CSV files for V2 devices are as follows:

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name,
snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password,
snmp_retries, snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v2,public,,,,,3,4
209.165.201.0,255.255.255.0,v2,public,,,,,3,4,Cisco,Cisco,2,10
```

Note The SNMP, telnet, or SSH credentials are mandatory.

The sample CSV files for V3 devices are as follows:

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type,
snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v3,default,HMAC-MD5,default,None,,3,4
209.165.201.0,255.255.255.224,v3,default1,HMAC-MD5,default1,DES,default1,3,4,Cisco,Cisco,2
,10
```

The CSV files can contain the following fields:

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- telnet_username

- telnet_password
- enable_password
- telnet_retries
- telnet_timeout

Removing Autonomous Access Points

To remove an autonomous access point from the NCS, follow these steps:

Step 1 Select the check boxes of the access points you want to remove.

Step 2 Choose **Remove APs** from the Select a command drop-down list.

Viewing Autonomous Access Points in the NCS

Once added, the autonomous access points can be viewed on the Monitor > Access Points page.

Click the autonomous access point to view more detailed information such as the following:

- Operational status of the access points
- Key attributes including radio information, channel, power, and number of clients on the radio
- CDP neighbored information

The autonomous access points can also be viewed in Monitor > Maps.

They can be added to a floor area by choosing **Monitor Maps >** *floor area* and choosing **Add Access Points** from the Select a command drop-down list.

Downloading Images to Autonomous Access Points (TFTP)

Lightweight access point images are bundled with controller images and managed by the controller. Autonomous access point images must be handled by a NMS system such as WLSE, CiscoWorks, or the NCS.

To download images to autonomous access points using TFTP, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Select the check box of the autonomous access point to which you want to download an image. The AP Type column displays whether the access point is autonomous or lightweight.

Step 3 From the Select a command drop-down list, choose **Download Autonomous AP Image (TFTP)**. The Download images to Autonomous APs page appears.

Step 4 Configure the following parameters:

- File is located on—Choose **Local machine** or **TFTP server**.
- Server Name—Choose the default server or add a new server from the Server Name drop-down list.
- IP address—Specify the TFTP server IP address. This is automatically populated if the default server is selected.
- NCS Server Files In—Specify where the NCS server files are located. This is automatically populated if the default server is selected.

- Server File Name—Specify the server filename.

Step 5 Click **Download**.

Tip Some TFTP servers might not support files larger than 32 MB.

Downloading Images to Autonomous Access Points (FTP)

To download images to autonomous access points (using FTP), follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Select the check box of the autonomous access point to which you want to download an image. The AP Type column displays whether the access point is autonomous or lightweight.

Step 3 From the Select a command drop-down list, choose **Download Autonomous AP Image (FTP)**. The Download images to Autonomous APs page appears.

Step 4 Enter the FTP credentials including username and password.

Step 5 Configure the following parameters:

- File is located on—Choose **Local machine** or **FTP server**.
- Server Name—Choose the default server or add a new server from the Server Name drop-down list.
- IP address—Specify the FTP server IP address. This is automatically populated if the default server is selected.
- NCS Server Files In—Specify where the NCS server files are located. This is automatically populated if the default server is selected.
- Server File Name—Specify the server filename.

Step 6 Click **Download**.

Supporting Autonomous Access Points in Work Group Bridge (WGB) mode

Workgroup Bridge (WGB) mode is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The WGB and its wired clients are listed as clients in the NCS if the AP mode is set to Bridge, and the access point is bridge capable.

To view a list of all the NCS clients that are WGBs, choose **Monitor > Clients**. From the Show drop-down list, choose **WGB Clients**, and click **Go**. The Clients (detected as WGBs) page appears. Click a user to view detailed information regarding a specific WGB and its wired clients.

Note The NCS provides WGB client information for the autonomous access point whether or not it is managed by the NCS. If the WGB access point is also managed by the NCS, the NCS provides basic monitoring functions for the access point similar to other autonomous access points.

Configuring Access Point Details

Choose **Configure > Access Points** to see a summary of all access points in the NCS database. The summary information includes the following:

- Ethernet MAC
- IP Address
- Radio
- Map Location
- AP Type
- Controller
- Operation Status
- Alarm Status
- Audit Status

Note If you hover your mouse cursor over the Audit Status value, the time of the last audit is displayed.

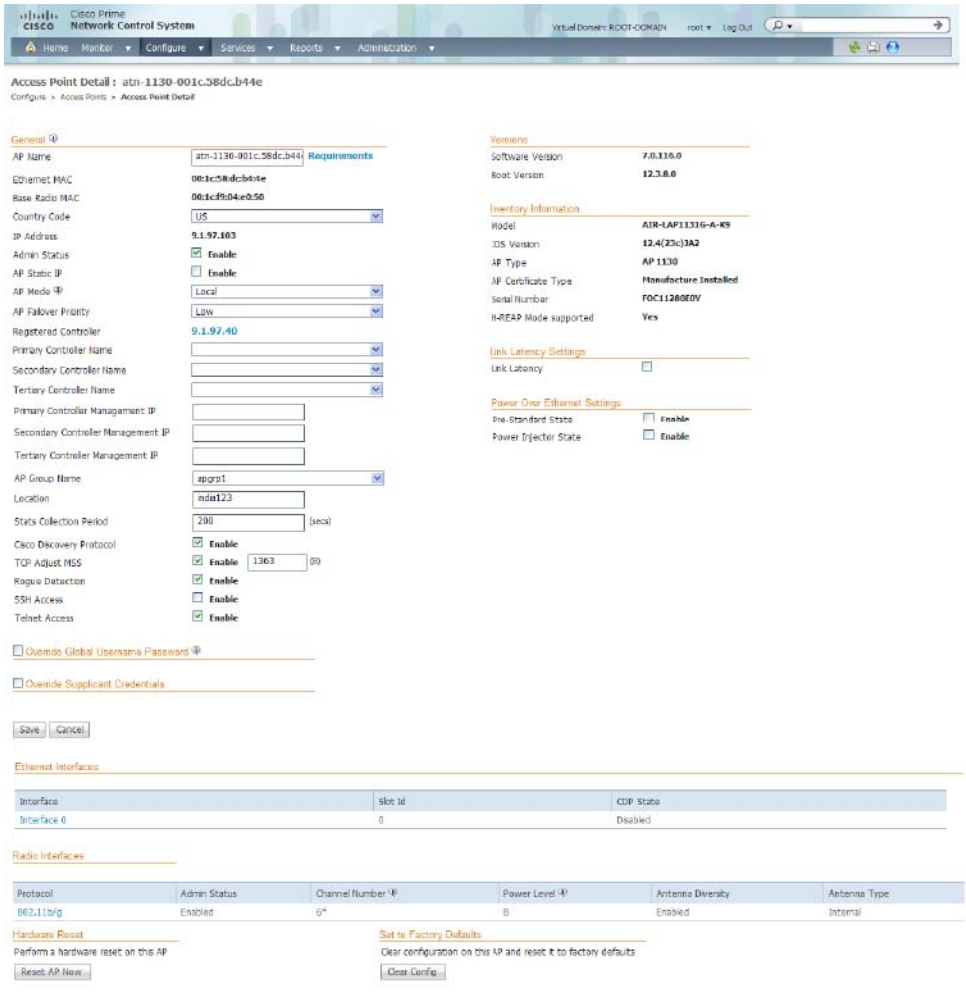
Note For details on configuring AP Configuration Templates, see "Configuring AP Configuration Templates" section on page 10-137.

Note You can click the **Edit View** link to add, remove or reorder columns such as AP Mode, Channel Width, Client Count, and so on. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Step 1 Click the link in the AP Name column to see detailed information about that access point name. The Access Point Detail page appears (see Figure 8-21).

Figure 8-21 Detailed Access Point Information

.



Note The operating system software automatically detects and adds an access point to the NCS database as it associates with existing controllers in the NCS database.

Note Access point parameters might vary depending on the access point type.

Some of the parameters on the page are automatically populated.

- The General group box displays the Ethernet MAC, the Base Radio MAC, IP Address, and status.
- The Versions group box of the page displays the software and boot version.
- The Inventory Information group box displays the model, AP type, AP certificate type, serial number, and REAP mode support.
- The Ethernet Interfaces group box provides information such as interface name, slot ID, admin status, and CDP state.

- The Radio Interfaces group box provides the current status of the 802.11a/n and 802.11b/g/n radios such as admin status, channel number, power level, antenna mode, antenna diversity, and antenna type.

To set the configurable parameters, follow these steps:

Note Changing access point parameters causes the access point to be temporarily disabled and this might cause some clients to lose connectivity.

Step 2 Enter the name assigned to the access point.

Step 3 Use the drop-down list to choose a country code to establish multiple country support. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that the access point complies with the regulations of your country. Consider the following when setting the country code:

- You can configure up to 20 countries per controller.
- Because only one auto-RF engine and one list of available channels exist, configuring multiple countries limits the channels available to auto-RF in the common channels. A common channel is one that is legal in each and every configured country.
- When you configure access points for multiple countries, the auto-RF channels are limited to the highest power level available in every configured country. A particular access point might be set to exceed these limitations (or you might manually set the levels in excess of these limitations), but auto-RF does not automatically choose a non-common channel or raise the power level beyond that available in all countries.

Note Access points might not operate properly if they are not designed for use in your country of operation. For example, an (-A) access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Europe (-E). Always be sure to purchase access points that match the regulatory domain of your country. For a complete list of country codes supported per product, see this URL:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html.

Step 4 If you want to enable the access point for administrative purposes, select the **Enable** check box.

Step 5 If you click **Enable** at the AP Static IP check box, a static IP address is always assigned to the access point rather than getting an IP address dynamically upon reboot.

Step 6 Choose the role of the access point from the AP Mode drop-down list. No reboot is required after the mode is changed *except* when monitor mode is selected. You are notified of the reboot when you click **Save**. The available modes are as follows:

- Local—This is the normal operation of the access point and the default AP Mode choice. With this mode, data clients are serviced while configured channels are scanned for noise and rogues. The access point goes off-channel for 50 ms and listens for rogues. It cycles through each channel for the period specified under the Auto RF configuration.
- FlexConnect—Choose **FlexConnect** from the AP Mode drop-down list to enable FlexConnect for up to six access points. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.

Note To configure Local or FlexConnect access points for Cisco Adaptive wIPS feature, choose Local or FlexConnect, and select the **Enhanced wIPS Engine Enabled** check box.

- Monitor—This is radio receive only mode and allows the access point to scan all configured channels every 12 seconds. Only deauthentication packets are sent in the air with an access point configured this way. A monitor mode access point detects rogues, but it cannot connect to a suspicious rogue as a client to prepare for the sending of RLDP packets.

Note You can expand the monitor mode for tags to include location calculation by enabling the tracking optimized monitor mode (TOMM) feature. When TOMM is enabled, you can specify which four channels within the 2.4 GHz band (802.11b/g radio) of an access point to use to monitor tags. This allows you to focus channel scans on only those channels for which tags are traditionally found (such as channels 1, 6, and 11) in your network. To enable TOMM, you must also make additional edits on the 802.11b/g radio of the access point. See the "Configuring Access Point Radios for Tracking Optimized Monitor Mode" section on page 8-194 for configuration details.

Note You cannot enable both TOMM and wIPS at the same time. TOMM can be enabled only when wIPS is disabled.

Note To configure access points for Cisco Adaptive wIPS feature, choose **Monitor** and select the **Enhanced wIPS Engine Enabled** check box, and select **wIPS** from the Monitor Mode Optimization drop-down list.

- Rogue Detector—In this mode, the access point radio is turned off, and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points expected. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.
- Sniffer—Operating in sniffer mode, the access point captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. These packets contain information such as timestamp, signal strength, packet size, and so on. This feature can only be enabled if you run AiroPeek, which is a third-party network analyzer software that supports the decoding of data packets. For more information on AiroPeek, see the following URL: www.wildpackets.com.
- Bridge—Bridge mode is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The bridge and its wired clients are listed as client in the NCS if the AP mode is set to Bridge, and the access point is bridge capable.
- SE-Connect—This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.

Note This option is displayed only if the access point is CleanAir-capable.

Note Changing the AP mode reboots the access point.

Step 7 Disable any access point radios.

Step 8 From the AP Failover Priority drop-down list, choose **Low**, **Medium**, **High**, or **Critical** to indicate the failover priority of the access point. The default priority is low. See the "Setting AP Failover Priority" section on page 8-162 for more information.

Step 9 In the Primary, Secondary, and Tertiary Controller fields, you can define the order in which controllers are accessed.

Step 10 The AP Group Name drop-down shows all access point group names that have been defined using WLANs > AP Group VLANs, and you can specify whether this access point is tied to any group.

Note An access point group name to 31 characters for WLC versions earlier than 4.2.132.0 and 5.0.159.0.

Step 11 Enter a description of the physical location where the access point was placed.

Step 12 In the Stats Collection Period field, enter the time in which the access point sends .11 statistics to the controller. The valid range is 0 to 65535 seconds. A value of 0 means statistics should not be sent.

Step 13 Choose **Enable** for Mirror Mode if you want to duplicate (to another port) all of the traffic originating from or terminating at a single client device or access point. Mirror mode is useful in diagnosing specific network problems but should only be enabled on an unused port since any connections to this port become unresponsive.

Step 14 You can globally configure MFP on a controller. When you do, management frame protection and validation are enabled by default for each joined access point, and access point authentication is automatically disabled. After MFP is globally enabled on a controller, you can disable and re-enable it for individual WLANs and access points.

If you click to enable MFP Frame Validation, three main functions are performed:

- Management frame protection—When management frame protection is enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing those receiving access points which were configured to detect MFP frames to report the discrepancy.
- Management frame validation—When management frame validation is enabled, the access point validates every management frame it receives from other access points in the network. When the originator is configured to transmit MFP frames, the access point ensures that the MIC IE is present and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE, it reports the discrepancy to the network management system. To report this discrepancy, the access point must have been configured to transmit MFP frames. Likewise, for the timestamps to operate properly, all controllers must be Network Transfer Protocol (NTP) synchronized.
- Event reporting—The access point notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and reports the results through SNMP traps to alert the network manager.

Step 15 Select the **Cisco Discovery Protocol** check box if you want to enable it. CDP is a device discovery protocol that runs on all Cisco-manufactured equipment, such as routers, bridges, and communication servers. Each device sends periodic messages to a multicast address and listens to the messages that others send to learn about neighboring devices. When the device boots, it sends a CDP packet specifying whether the device is inline power enabled so that the requested power can be supplied.

Note Changing access point parameters temporarily disables an access point and might result in loss of connectivity to some clients.

Step 16 Select the check box to enable rogue detection. See the "Rogue Access Point Location, Tagging, and Containment" section on page 3-13 for more information on rogue detection.

Note Rogue detection is disabled automatically for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. For more information regarding OfficeExtend access points, see the *Cisco Wireless LAN Controller Configuration Guide*.

Step 17 Select the **Encryption** check box to enable encryption.

Note Enabling or disabling encryption functionality causes the access point to reboot, which then causes clients to lose connectivity.

Note DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security, but disabled by default for all other access points.

Note Cisco 5500 controllers can be loaded with one of the two types of images, AS_5500_LDPE_x_x_x_x.aes or AS_5500_x_x_x_x.aes. For the 5500 controller loaded with former image, you need to have DTLS License to show encryption.

Note For WiSM2 and 2500 controllers, it is mandatory to have DTLS license to show encryption.

Step 18 If rogue detection is enabled, the access point radio is turned off, and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points expected. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.

Step 19 Select the **SSH Access** check box to enable SSH access.

Step 20 Select the **Telnet Access** check box to enable Telnet access.

Note An OfficeExtend access point might be connected directly to the WAN which allows external access if the default password is used by the access point. Therefore, Telnet and SSH access are disabled automatically for OfficeExtend access points.

Step 21 If you want to override credentials for this access point, select the **Override Global Username Password** check box. You can then enter a new supplicant AP username, AP password, and Enable password that you want to assign for this access point.

Note In the System > AP Username Password page, you can set global credentials for all access points to inherit as they join a controller. These established credentials appear in the lower right of the AP Parameters tab page.

The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

Step 22 Select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. See the "Configuring Link Latency Settings for Access Points" section on page 8-213 for more information on link latency.

Step 23 You can now manipulate power injector settings through the NCS without having to go directly to the controllers. In the Power Over Ethernet Settings section, select the check box to enable pre-standard or power injector state.

Pre-standard is chosen if the access point is powered by a high power Cisco switch; otherwise, it is disabled. If power injector state is selected, power injector options appear. The possible values are installed or override. If you choose override, you can either enter a MAC address or leave it empty so that it is supplied by WLC.

Note To determine which source of power is running the NCS, choose **Monitor > Access Points**, click **Edit View**, and then choose and move POE Status to the View Information box. After you click **Submit**, the POE status appears in the last column. If the device is powered by an injector, the POE status appears as Not Applicable.

Step 24 Select the **Enable** check box to enable the following FlexConnect configurations:

Note FlexConnect settings cannot be changed when the access point is enabled.

- OfficeExtend AP—The default is Enabled.

  Note Unselecting the check box simply disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point, but it does put the access point at risk because it becomes remotely deployed. If you want to clear the configuration of an access point and return it to factory default settings, click **Clear Config** at the bottom of the access point details page. If you want to clear only the personal SSID of the access point, click **Reset Personal SSID** at the bottom of the access point details page.

When you select Enabled for the OfficeExtend AP, a warning message provides the following information:

- Configuration changes that automatically occur. Encryption and Link Latency are enabled. Rogue Detection, SSH Access, and Telnet Access are disabled.
- A reminder to configure at least one primary, secondary, and tertiary controller (including name and IP address).

Note Typically, an access point first looks for the primary controller to join. After that, the controller tries the secondary and then the tertiary controller. If none of these controllers are configured, the access point switches to a default discovery mode in an attempt to join whatever controller it might find.

An OfficeExtend access point searches only for a primary, secondary, or tertiary controller to join. It does not look any further for a configured controller. Because of this, it is important that you configure at least one primary, secondary, or tertiary controller name and IP address.

  - A warning the enabling encryption causes the access point to reboot and causes clients to lose connectivity.

- Least Latency Controller Join—When enabled, the access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.

Note The access point only performs this search once when it initially joins the controller. It does not recalculate the primary, secondary, and tertiary controllers latency measurements once joined to see if the measurements have changed.

- VLAN Support—When selected, enter the Native VLAN identifier.

  When Enable VLAN is selected, the NCS displays locally switched VLANs. You can only edit a VLAN ID that is mapped to a WLAN ID.

- AP level VLAN ACL Mapping—This group box appears only for FlexConnect mode access points with VLAN support enabled.You can only edit the Ingress and Egress ACLs mapped to a VLAN ID.

Note The AP level VLAN ACL Mapping configuration is pushed to the access point, only when the VLAN IDs entered in the NCS is available in the AP Level VLAN ACL Mapping section of the access point in the associated controller.

- Group level VLAN ACL Mapping—This group box appears only for FlexConnect mode access points with VLAN support enabled.You can view the Group level VLAN ACL mapping that you have specified under the ACL tab of the FlexConnect ACL groups.
- PreAuthentication ACL Mappings
  - Web-Authentication and Web-Policy ACLs—Click the **External WebAuthentication ACLs** link to view the WebAuth and Web Policy ACL mappings at access point level. The ACL Mappings page lists details of the WLAN ACL mappings and web policy ACLs.

Step 25 Select the role of the mesh access point from the Role drop-down list. The default setting is MAP.

Note An access point in a mesh network functions as either a root access point (RAP) or mesh access point (MAP).

Step 26 Enter the name of the bridge group to which the access point belongs. The name can have up to 10 characters.

Note Bridge groups are used to logically group the mesh access points to avoid two networks on the same channel from communicating with each other.

Note For mesh access points to communicate, they must have the same bridge group name.

Note For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another.

Note For configurations where separate sectors are required, make sure that each RAP and its associated MAPs have separate bridge group names.

The Type field appears whether the mesh access point is an indoor or outdoor access point, and the Backhaul Interface field displays the access point radio that is being used as the backhaul for the access point.

Step 27 Choose the data rate for the backhaul interface from the drop-down list. Data rates available are dictated by the backhaul interface. The default rate is 18 Mbps.

Note This data rate is shared between the mesh access points and is fixed for the whole mesh network.

Note Do NOT change the data rate for a deployed mesh networking solution.

Step 28 Choose **Enable** from the Ethernet Bridging drop-down list to enable Ethernet bridging for the mesh access point.

Step 29 Click **Save** to save the configuration.

Step 30 Re-enable the access point radios.

Step 31 If you need to reset this access point, click **Reset AP Now**.

Step 32 Click **Reset Personal SSID** to reset the OfficeExtend access point personal SSID to the factory default.

Step 33 If you need to clear the access point configuration and reset all values to the factory default, click **Clear Config**.

Configuring an Ethernet Interface

Note The 152x mesh access points are configured on any one of these four ports: port 0-PoE in, port 1-PoE out, Port 2 - cable, and port 3- fiber. Other APs (such as 1130,1140,1240,1250) are configured on Port 2 - cable.

To configure an Ethernet interface, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Click the link under AP Name to see detailed information about that access point name. The Access Point Detail page appears.

Note The Access Point Details page displays the list of Ethernet interfaces.

Step 3 Click the link under Interface to see detailed information about that interface. The Ethernet Interface page appears.

This page displays the following parameters:

- AP Name—The name of the access point.
- Slot Id—Indicates the slot number.
- Admin Status—Indicates the administration state of the access point.
- CDP State—Select the **CDP State** check box to enable the CDP state.

Step 4 Click **Save**.

Importing AP Configuration

To import a current access point configuration file, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 From the **Select a command** drop-down list, choose **Import AP Config**.

A pop-up aleart box appears stating All Unified AP(s) are imported from CSV file only. Unified AP(s) from Excel and XML file are not imported.

Step 3 Click **OK** to close the pop-up alert box.

Step 4 Click **Go**.

Step 5 Enter the CSV file path in the text box or click **Browse** to navigate to the CSV file on your computer.

The first row of the CSV file is used to describe the columns included. The AP Ethernet Mac Address column is mandatory. The parameters on this page are used for columns not defined in the CSV file.

Sample File Header:

ethernetMac,apName,location,primaryController,secondaryController,tertiaryController

00:1c:58:74:8c:22, ap-1, sjc-14-a, controller-4404-1, controller-4404-2, controller-4404-3

- ethernetMac—Access point Ethernet MacAddress
- apName—Access point name
- location—Access point location
- primaryController—Primary Controller
- secondaryController—Secondary Controller
- tertiaryController—Tertiary Controller

The CSV file can contain the following fields:

- AP Ethernet MacAddress—Mandatory
- AP Name—Optional
- Location—Optional
- Primary Controller—Optional
- Secondary Controller—Optional
- Tertiary Controller—Optional

Note Optional fields can remain empty. The AP Config Import ignores empty optional field values. However, if primaryMwar and secondaryMwar entries are empty then a unified access point update is not complete.

Step 6 When the appropriate CSV file path appears in the Select CSV File text box, click **OK**.

Exporting AP Configuration

To export current access point configuration files, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 From the Select a command drop-down list, choose **Export AP Config**.

A pop-up alert box appears stating All Unified AP(s) are exported to CSV/EXCEL/XML file.

Step 3 Click **OK** to close the pop-up alert box.

Step 4 Click **Go** to view the current AP configurations including:

- apName
- ethernetMac
- location
- primaryController
- secondaryController
- tertiaryController

Step 5 Select the file option (CSV, Excel, XML) to export the access point configurations.

Step 6 In the File Download window, click **Save** to save the file.

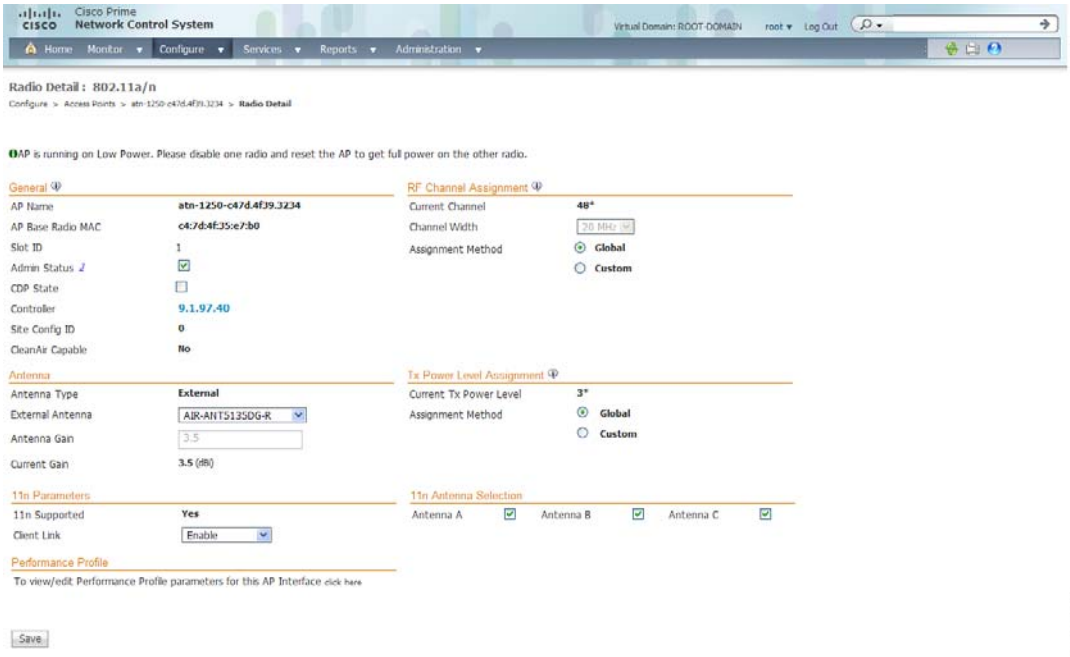
Configuring Access Points 802.11n Antenna

The NCS provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

Note At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

If you choose **Configure > Access Points** and select an **802.11n** item from the Radio column, the following page appears (see Figure 8-22).

Figure 8-22 Access Point > 802.11a/n



This page contains the following fields:.

Note Changing any of the fields causes the radio to be temporarily disabled and thus might result in loss of connectivity for some clients.

General

- AP Name—The operator-defined name of the access point.
- AP Base Radio MAC—MAC address of the base radio of the access point.
- Admin Status—Select the box to enable the administration state of the access point.
- CDP State—Select the **CDP State** check box to enable CDP.
- Controller—IP address of the controller. Click the IP address of the controller for more details.
- Site Config ID—Site identification number.
- CleanAir Capable—Displays if the access point is CleanAir capable.
- CleanAir—Select the check box to enable CleanAir.

Antenna

- Antenna Type—Indicates an external or internal antenna.
- Antenna Diversity—Select **Right**, **Left**, or **Enabled**.

Note Antenna diversity refers to the Cisco Aironet access point feature where an access point samples the radio signal from two integrated antenna ports and choose the preferred antenna. This diversity option is designed to create robustness in areas with multi-path distortion.

For external antenna, select one of the following:

  - Enabled—Use this setting to enable diversity on both the left and right connectors of the access point.
  - Left—Use this setting if your access point has removable antennas and you install a high-gain antenna on the left connector of the access point.
  - Right—Use this setting if your access point has removable antennas and you install a high-gain antenna on the right connector of the access point.

For internal antennas, select one of the following:

  - Enabled—Use this setting to enable diversity on both Side A and Side B.
  - Side A—Use this setting to enable diversity on Side A (front antenna) only.
  - Side B—Use this setting to enable diversity on Side B (rear antenna) only.
- External Antenna—Choose the **external antenna** or **Other** from the drop-down list.
- Antenna Gain—Enter the desired antenna gain in the text box.

Note The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.

- Current Gain (dBm)—Indicates the current gain in dBm.

Table 8-4 lists the antenna names, gain, and descriptions.

Table 8-4 Antenna Names, Gain, and Descriptions

Antenna Name	Gain (dBi)	Description
AIR-ANT1000	0.00	AP 1000 Integrated antenna
CUSH-S5157WP	3.00	5.15-5.87 GHz diversity wideband panel antenna (side gain and back attenuation)
KODIAK-DIRECTIONAL	8.00	Integrated Kodiak directional antenna
KODIAK-OMNI	5.00	Kodiak omni antenna
AIR-ANT1728	5.20	Omni ceiling mount antenna
AIR-ANT1729	6.00	Patch wall mount antenna
AIR-ANT2012	6.50	Diversity patch wall mount antenna
AIR-ANT2410Y-R	10.00	Yagi master or wall mount antenna
AIR-ANT5959	2.00	Omni diversity ceiling mount antenna

Table 8-4 Antenna Names, Gain, and Descriptions (continued)

Antenna Name	Gain (dBi)	Description
AJAX-OMNI	5.00	Integrated Ajax omni antenna
AIR-ANT5135D-R	3.50	Omni dipole antenna
AIR-ANT5135DW-R	3.50	3.5-dBi white dipole antenna
AIR-ANT5135DG-R	3.50	3.5 dB5 gray non-articulating dipole antenna
AIR-ANT2422DW-R	2.20	2.2-dBi white dipole antenna
AIR-ANT2422DB-R	2.20	Omni dipole antenna
AIR-ANT2422DG-R	2.20	2.2 dBi gray non-articulating dipole antenna
AIR-ANT5145V-R	4.50	Omni diversity antenna
AIR-ANT5160V-R	6.00	Omni antenna
AIR-ANT3549	9.00	Patch wall mount antenna
AIR-ANT4941	2.20	Omni dipole antenna
AIR-ANT2506	0.00	Omni mass mount antenna
AIR-ANT3213	5.20	Omni diversity pillar antenna
CUSH-S24516DBP	3.00	Integrated 2.4/5 GHz hemispheric pattern
CUSH-S5153WBPX	6.00	Ceiling mount 6-dBi omni
AIR-ANT5170V-R	7.00	Wall mount diversity patch antenna
AIR-ANT5175V	7.50	Omni antenna for Wireless Bridge
AIR-ANT5195V-R	9.50	Wall mount patch antenna
AIR-ANT58G10SSA	9.50	Sector antenna for Wireless Bridge
AIR-ANT2455V	5.50	Omni antenna for Wireless Bridge
CUSH-S54717P	17.00	Patch array antenna for Wireless Bridge
CUSH-S49014WP	14.00	Patch array antenna for Wireless Bridge
CUSH-S2406BP	8.00	Omni antenna for Wireless Bridge
AIR-ANT1100	2.20	Default antenna for AP1100
BR1310	13.00	Integrated patch directional antenna
AIR-ANT2460	6.00	Patch wall mount antenna
AIR-ANT2465	6.50	Diversity patch wall mount antenna
AIR-ANT2485	9.00	Patch wall mount antenna
AIR-ANT2480V-N	8.00	2.4 GHz omni antenna for mesh
AIR-ANT5114P-N	14.00	5 GHz patch for mesh
AIR-ANT5117S-N	17.00	5 GHz sector for mesh
AIR-ANT2450V-N	5.00	2.4 GHz omni antenna
AIR-ANT5180V-N	8.00	5 GHz omni antenna
AIR-ANT2450S-R	5.50	2.4 GHz 135-degree sector antenna

Table 8-4 Antenna Names, Gain, and Descriptions (continued)

Antenna Name	Gain (dBi)	Description
AIR-ANT2451V-R	2.4 GHz—2.0 5 GHz—3.0	2.4 GHz and 5 GHz four-element dual band antenna. **Note** Two elements for the 2.4 GHz band and two elements for the 5 GHz band.
AIR-ANT2460NP-R	6.00	2.4 GHz MIMO (3-Element) Patch Antenna
AIR-ANT5160NP-R	6.00	5 GHz MIMO (3-Element) Patch Antenna
AIR-ANT2422SDW-R	2.20	2.4 GHz “Stubby” white monopole antenna
AIR-ANT5135SDW-R	3.50	5 GHz "Stubby" white monopole antenna
AIR-ANT2451NV-R	2.4 GHz—2.5 5 GHz—3.5	2.4 GHz and 5 GHz “6-pack” ceiling mount omni antenna
AIR-ANT2452V-R	5.2	2.4 GHz Diversity Wall Mount Omni-directional Antenna **Note** This is a replacement antenna to the existing AIR-ANT3213.
AIR-ANT24020V-R	2.0	External omni diversity ceiling mount antenna **Note** This is a replacement antenna to the existing antenna AIR-ANT5959.
AIR-ANT2547V-N	2.4 GHz—4.0 5 GHz—7.0	2.4 GHz and 5 GHz dual band Omni-directional Antenna.

Table 8-5 lists the default values of some of the attributes of an access point when it is added to the NCS for the first time.

Table 8-5 Supported Antennas

AP Type	Radio Type	Supported Antennas
AP 1200	802.11a	KODIAC-OMNI, KODIAK-DIRECTIONAL, AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R
	802.11b/g	AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1240	802.11a	AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R
	802.11b/g	AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1131	802.11a	AJAX-OMNI
	802.11b/g	AJAX-OMNI

Table 8-5 Supported Antennas (continued)

AP Type	Radio Type	Supported Antennas
AP 1100	802.11b/g (only b/g)	AIR-ANT1100
AP 1310	802.11a	AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R
	802.11b/g	BR1310, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1250	802.11a	AIR-ANT5135D-R, AIR-ANT5135SDW-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5160NP-R, AIR-ANT5170V-R, AIR-ANT5195V-R, AIR-ANT2451NV-R-5GHz
	802.11b/g	AIR-ANT2460, AIR-ANT2460NP-R, AIR-ANT2422SDW-R, AIR-ANT2451NV-R-2.4GHz, AIR-ANT2465, AIR-ANT2485, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1000	802.11a	AIR-ANT1000, AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R, CUSH-S5157WP, CUSH-S24516DBP
	802.11b/g	AIR-ANT1000, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT5959, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, CUSH-S24516DBP, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1030	802.11a	AIR-ANT1000, AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R, CUSH-S5157WP, CUSH-S24516DBP
	802.11b/g	AIR-ANT1000, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT5959, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, CUSH-S24516DBP, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1500	802.11a	AIR-ANT5175V, AIR-ANT58G10SSA, CUSH-S54717P, CUSH-S49014WP
	802.11b/g	AIR-ANT2455V, CUSH-S2406BP
AP 1505	802.11a	AIR-ANT5175V, AIR-ANT58G10SSA, CUSH-S54717P, CUSH-S49014WP
	802.11b/g	AIR-ANT2455V, CUSH-S2406BP
AP 1260	802.11a	AIR-ANT5135DG-R, AIR-ANT5135D-R, AIR-ANT5135DB-R, AIR-ANT5135DW-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R, AIR-ANT5140V-R, AIR-ANT2451V-R, AIR-ANT2450S-R, AIR-ANT5135SDW-R, AIR-ANT2451NV-R-5GHz, AIR-ANT5160NP-R

Table 8-5 Supported Antennas (continued)

AP Type	Radio Type	Supported Antennas
	802.11b/g	AIR-ANT2422DG-R, AIR-ANT4941, AIR-ANT2422DB-R, AIR-ANT2422DW-R, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2430V-R, AIR-ANT24120, AIR-ANT2414S-R, AIR-ANT1949, AIR-ANT2451V-R, AIR-ANT2450S-R, AIR-ANT2460NP-R, AIR-ANT2422SDW-R, AIR-ANT2451NV-R-2.4GHz, AIR-ANT24020V-R, AIR-ANT2452V-R
AP 1040	802.11a	Internal-1040-5.0 GHz
	802.11b/g	Internal-1040-2.4 GHz
AP 1140	802.11a	Internal-1140-5.0 GHz
	802.11b/g	Internal-1140-2.4 GHz
AP 1550	802.11a	AIR-ANT2547V-N-5.0GHz, Internal-1550-5.0 GHz
	802.11b/g	AIR-ANT2547V-N-2.4GHz,Internal-1550-2.4GHz
AP 3500e	802.11a	AIR-ANT5135DG-R,AIR-ANT5135D-R,AIR-ANT5135DB-R,AIR-ANT5135DW-R,AIR-ANT5145V-R,AIR-ANT5160V-R,AIR-ANT5170V-R,AIR-ANT5195V-R,AIR-ANT5140V-R,AIR-ANT2451V-R,AIR-ANT2450S-R,AIR-ANT5135SDW-R,AIR-ANT2451NV-R-5GHz,AIR-ANT5160NP-R
AP 3500e	802.11b/g	AIR-ANT2422DG-R,AIR-ANT4941,AIR-ANT2422DB-R,AIR-ANT2422DW-R,AIR-ANT2460,AIR-ANT2465,AIR-ANT2485,AIR-ANT1728,AIR-ANT2012,AIR-ANT1729,AIR-ANT2410Y-R,AIR-ANT5959,AIR-ANT3549,AIR-ANT2506,AIR-ANT3213,AIR-ANT2430V-R,AIR-ANT24120,AIR-ANT2414S-R,AIR-ANT1949,AIR-ANT2451V-R,AIR-ANT2450S-R,AIR-ANT2460NP-R,AIR-ANT2422SDW-R,AIR-ANT2451NV-R-2.4GHz,AIR-ANT24020V-R,AIR-ANT2452V-R
AP 3500i	802.11a	Internal-3500i-5 GHz
AP 3500i	802.11b/g	Internal-3500i-2.4 GHz
AP 3600e	802.11a	AIR-ANT2524DB-R, AIR-ANT2524DW-R, AIR-ANT2524DG-R, AIR-ANT2566P4W-R, AIR-ANT2524V4C-R.
AP 3600e	802.11b/g	AIR-ANT2524DB-R, AIR-ANT2524DW-R, AIR-ANT2524DG-R, AIR-ANT2566P4W-R, AIR-ANT2524V4C-R.
AP 3600i	802.11a	Internal-3600i-5 GHz
AP 3600i	802.11b/g	Internal-3600i-2.4 GHz
AP 3500p	802.11a	AIR-ANT5135DG-R, AIR-ANT5135D-R, AIR-ANT5135DW-R, AIR-ANT5140V-R, AIR-ANT5135SDW-R, AIR-ANT5160NP-R
AP 3500p	802.11b/g	AIR-ANT2422DG-R, AIR-ANT2422DB-R, AIR-ANT2422DW-R, AIR-ANT1728, AIR-ANT2410Y-R, AIR-ANT2506, AIR-ANT2430V-R, AIR-ANT1949, AIR-ANT2450S-R, AIR-ANT2460NP-R, AIR-ANT2451NV-R-2.4GHz, AIR-ANT2440NV-R, AIR-ANT2460P-R, AIR-ANT2485P-R

Table 8-5 Supported Antennas (continued)

AP Type	Radio Type	Supported Antennas
801GN	802.11a	Not Applicable
	802.11b/g	AIR-ANT4941, AIR-ANT2422DB-R
801AGN	802.11a	AIR-ANTM2050D-R
	802.11b/g	AIR-ANTM2050D-R
802GN	802.11a	Not Applicable
	802.11b/g	Internal-802.11
802AGN	802.11a	AIR-ANTM2050D-R
	802.11b/g	AIR-ANTM2050D-R

WLAN Override

The following 802.11a WLAN Override field appears:

- WLAN Override—Choose **Enable** or **Disable** from the drop-down list.

Note When you enable WLAN Override, operating system displays a table showing all current Cisco WLAN Solution WLANs. In the table, select WLANs to enable WLAN operation, and deselect WLANs to disallow WLAN operation for this 802.11a Cisco Radio.

Note WLAN override does not apply to access points that support the 512 WLAN feature.

Performance Profile

Click the URL to view or edit performance profile parameters for this access point interface.

- ClientLink—Enable or disable client link for the access point radios per interface. This feature is only supported for legacy (orthogonal frequency-division multiplexing) OFDM rates. The interface must support ClientLink, and OFDM rates must be enabled. Also, two or more antennas must be enabled for transmission, and all three antennas must be enabled for reception.

Note The maximum number of clients supported is 15. If the antenna configuration restricts operation to a single transmit antenna or OFDM rates are disabled, ClientLink cannot be used.

RF Channel Assignment

The following 802.11a RF Channel Assignment parameters appear:

- Current Channel—Channel number of the access point.
- Assignment Method—Select one of the following:
  - Global—Use this setting if the channel of the access point is set globally by the controller.
  - Custom—Use this setting if the channel of the access point is set locally. Select a channel from the drop-down list.

For example, if you select 2(17 dBm) as the custom power, 2 corresponds to the Power Level and 17 is the Absolute Power (dBm).

- Channel width—Select the channel width from the drop-down list. The selections include 20, above 40, and below 40.

  RF Channel assignment supports 802.11n 40 MHz channel width in the 5-GHz band. 40-MHz channelization allows radios to achieve higher instantaneous data rates.

Note Selecting a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments.

Note The power level and channel numbers of an access point are not audited.

Tx Power Level Assignment

- Current Tx Power Level—Indicates the current transmit power level.
- Assignment Method—Select one of the following:
  - Global—Use this setting if the power level is set globally by the controller.
  - Custom—Use this setting if the power level of the access point is set locally. Choose a power level from the drop-down list.

11n Antenna Selection

The NCS provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

Note At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

Select any of the 11n Antenna Selection parameters:

- Antenna A
- Antenna B
- Antenna C
- Antenna D

11n Parameters

The following 11n fields appear:

- 11n Supported—Indicates whether or not 802.11n radios are supported.
- Client Link—Use this option to enable or disable client links. Choose **Enable**, **Disable**, or **Not Applicable** from the drop-down list.

Configuring CDP

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

Note CDP is enabled on the Ethernet and radio ports of the bridge by default.

Configuring CDP on Access Points

To configure CDP on Radio or Ethernet interfaces, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Choose an access point associated with software release 5.0 or later.

Step 3 Click the slots of radio or an Ethernet interface for which you want to enable CDP.

Step 4 Select the **CDP State** check box to enable CDP on the interface.

Step 5 Click **Save**.

Configuring Access Point Radios for Tracking Optimized Monitor Mode

To optimize monitoring and location calculation of tags, you can enable Tracking Optimized Monitor Mode (TOMM) on up to four channels within the 2.4-GHz band (802.11b/g radio) of an access point. This allows you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

After enabling Monitor mode at the access point level, you must then enable TOMM and assign monitoring channels on the 802.11b/g radio of the access point.

Note For details on enabling Monitor mode on an access point, see Step 6 in the "Configuring Access Point Details" section on page 8-174.

To set enable TOMM and assign monitoring channels on the access point radio, follow these steps:

Step 1 After enabling Monitor mode at the access point level, choose **Configure > Access Points**.

Step 2 In the Access Points page, click the **802.11 b/g Radio** link for the appropriate access point.

Step 3 In the General group box, disable **Admin Status** by unselecting the check box. This disables the radio.

Step 4 Select the **TOMM** check box. This check box only appears for Monitor Mode APs. The drop-down lists for each of the four configurable channels are displayed.

Step 5 Choose the four channels on which you want the access point to monitor tags.

Note You can configure fewer than four channels for monitoring. To eliminate a monitoring channel, choose **None** from the channel drop-down list.

Step 6 Click **Save**. Channel selection is saved.

Step 7 In the Radio parameters page, reenable the radio by selecting the **Admin Status** check box.

Step 8 Click **Save**. The access point is now configured as a TOMM access point.

The AP Mode displays as Monitor/TOMM in the Monitor > Access Points page.

Copying and Replacing Access Points

The Copy and Replace AP feature is useful if you need to remove an access point from the network and replace it with a new access point. All of the access point information, such as AP mode, name, and map location needs to be copied from the old access point to the new access point.

To access the **Copy and Replace AP** function, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Select the check box for the applicable access point.

Step 3 From the Select a command drop-down list, choose **Copy and Replace AP**.

Step 4 Click **Go**.

The old access point needs to be removed from the network first. This access point then becomes unassociated to any controller.When you plug in the new access point, it is associated with the controller and the NCS refreshes the information. At that point, select the old unassociated access point and choose to copy and replace the configuration to the new access point.

Note If a different access point type is used to replace an older access point, only the configuration parameters that apply are copied.

Removing Access Points

To remove access points that are not associated, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 From the Select a command drop-down list, choose **Remove APs**.

Step 3 Click **Go**.

Step 4 Click **OK** to confirm the removal.

Scheduling and Viewing Radio Status

This section contains the following topics;

Scheduling Radio Status

To schedule a radio status change (enable or disable), follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Select the check box for the applicable access point(s).

Step 3 From the Select a command drop-down list, choose **Schedule Radio Status**.

Step 4 Click **Go**.

Step 5 Choose **Enable** or **Disable** from the Admin Status drop-down list.

Step 6 Use the Hours and Minutes drop-down lists to determine the scheduled time.

Step 7 Click the calendar icon to select the scheduled date for the status change.

Step 8 If the scheduled task is recurring, choose **Daily** or **Weekly**, as applicable. If the scheduled task is a one-time event, choose **No Recurrence**.

Step 9 Choose **Save** to confirm the scheduled task.

Viewing Scheduled Tasks

To view currently scheduled radio status tasks, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Select the check box for the applicable access point(s).

Step 3 From the Select a command drop-down list, choose **View Scheduled Radio Task(s)**.

Step 4 Click **Go**.

The Scheduled Task(s) information includes:

- Scheduled Task(s)—Choose the task to view its access points and access point radios.
- Scheduled Radio adminStatus—Indicates the status change (Enable or Disable).
- Schedule Time—Indicates the time the schedule task occurs.
- Execution status—Indicates whether or not the task is scheduled.
- Recurrence—Indicates Daily or Weekly if the scheduled task is recurring.
- Next Execution—Indicates the time and date of the next task occurrence.
- Last Execution—Indicates the time and date of the last task occurrence.
- Unschedule—Click **Unschedule** to cancel the scheduled task. Click **OK** to confirm the cancellation.

Viewing Audit Status (for Access Points)

An Audit Status column in the Configure > Access Points page shows an audit status for each of the access points. You can also view the audit report for the selected access points. The report shows the time of the audit, the IP address of the selected access point, and the synchronization status.

To view the audit status, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Click the **Audit Status** column value to go to the latest audit details page for the selected access point. This report is interactive and per access point.

Note If you hover your mouse cursor over the Audit Status column value, the time of the last audit is displayed.

To run an access point on-demand audit report, select the desired access point for which you want to run the report and choose **Audit Now** from the Select a command drop-down list. In versions prior to 4.1, the audit only spanned the parameters present in the AP Details and AP Interface Details page. In Release 4.1, this audit report covers complete access point level auditing. The audit results are stored in the database so that you can view the latest audit reports without having to run another audit.

Note The audit can only be run on an access point that is associated to a controller.

Filtering Alarms for Maintenance Mode Access Points

The NCS uses critical alarms to track if the managed access points are down. The controller sends three different alarms when the following occurs:

- The Access point is down
- Radio A of the access point is down
- Radio B/G of the access point is down

In Release 7.0.172.0 and later, these 3 alarms are grouped into a single alarm.

When an access point is under technical maintenance, the critical alarms need to be deprioritized. You can deprioritize the severity of an alarm of an access point using the Configure > Access Points page. When you move an access point to maintenance state, the alarm status for that access point appears in black color.

This section contains of the following topics:

Placing an Access Point in Maintenance State

To move an access point to the maintenance state, follow these steps:

Step 1 Choose **NCS > Configure > Access Points**.

The Access Points page appears.

Step 2 From the drop-down list, choose **Place in Maintenance State**, and click **Go**.

The access point is moved to maintenance state.

Once the access point is moved to maintenance state, the access point down alarms are processed with lower severity instead of critical.

Removing an Access Point from Maintenance State

To remove an access point from the maintenance state, follow these steps:

Step 1 Choose **NCS > Configure > Access Points**.

The Access Points page appears.

Step 2 From the drop-down list, choose **Remove from Maintenance State**, and click **Go**.

The access point is removed from the maintenance state.

Searching Access Points

Use the search options in the uppermost right corner of the page to create and save custom searches:

- New Search: Enter an IP address, name, SSID, or MAC, and click **Search**.
- Saved Searches: Click **Saved Search** to choose a category, a saved custom search, or choose other criteria for a search from the drop-down lists.
- Advanced Search: An advanced search allows you to search for a device based on a variety of categories and filters.

See the "Using the Search Feature" section on page 2-33 for further information.

After you click **Go**, the access point search results appear (see Table 8-6).

Table 8-6 Access Point Search Results

Field	Options
IP Address	IP address of the access point.
Ethernet MAC	MAC address of the access point.
AP Name	Name assigned to the access point. Click the access point name item to display details.
Radio	Protocol of the access point is either 802.11a/n or 802.11b/g/n.
Map Location	Campus, building, and floor location.
Controller	IP address of the controller.
AP Type	Access point radio frequency type.
Operational Status	Displays the operational status of the Cisco radios (Up or Down).

Table 8-6 Access Point Search Results (continued)

Alarm Status	Alarms are color coded as follows: • Clear = No Alarm • Red = Critical Alarm • Orange = Major Alarm • Yellow = Minor Alarm
Audit Status	The audit status of the access point.
Serial Number	The serial number of the access point.
AP Mode	Describes the role of the access point modes such as Local, FlexConnect, Monitor, Rogue Detector, Sniffer, Bridge, or SE-Connect.

Viewing Mesh Link Details

You can access mesh link details in several ways:

- Click the **Mesh** dashboard in the NCS home page
- Choose **Monitor > Access Points**, click the **Mesh Links** tab and then click the **Details** link
- After you import a KML file from Google Earth, click the **AP Mesh** link

The current statistics are displayed at the top of the page followed by diagrams for certain statistics.

- SNR Graph—SNR Up and Down graphs are combined into one graph. Each set of data is represented by different colors.
- Link Metrics Graph—The Adjusted Link Metric and Unadjusted Link Metric is combined into one graph. Each set of data is represented by different colors.
- Packet Error Rate Graph—Displays the packet error rates in a graph.
- Link Events—The last five events for the link are displayed.
- Mesh Worst SNR Links—Displays the worst signal-to-noise ratio (SNR) links.
- AP Uptime—These statistics help determine if an access point is rebooting frequently.
- LWAPP Join Taken Time—These statistics determine how long it takes an access point to join.
- Location Links—Allows you to navigate to the NCS map or the Google Earth location.

Viewing or Editing Rogue Access Point Rules

You can view or edit current rogue access point rules on a single WLC. See the "Configuring a Rogue AP Rules Template" section on page 10-83 for more information.

To access the rogue access point rules, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

Step 3 From the left sidebar menu, choose **Security > Rogue AP Rules**. The Rogue AP Rules displays the rogue access point rules, the rule types (malicious or friendly), and the rule sequence.

Step 4 Choose a Rogue AP Rule to view or edit its details.

Configuring Switches

You can add switches to the NCS database to view overall switch health and endpoint monitoring and to perform switchport tracing. While this switch functionality appears on the Configuration menu in the NCS, you are configuring the NCS system and not the switches. You cannot configure switch features using the NCS.

The NCS allows you to do the following:

- Add switches in Configure > Switches page and specify CLI and SNMP credentials. See the "Adding Switches" section on page 8-203 for more information.
- Monitor Switches by choosing Monitor > Switches. See the "Monitoring Switches" section on page 5-33 for more information.
- Run switch-related reports using the Reports menu.

Note In the Configure > Switches page, you can also add a location-capable switch for tracking wired clients by mobility services engine and the NCS.

This section contains the following topics:

Note The following switches are supported: 3750, 3560, 3750E, 3560E, and 2960.

Features Available by Switch Type

When you add a switch to the NCS, you specify how the switch is to be managed. Based on how you specify the switch is to be managed, the NCS determines which features are available:

- Monitored switches—You can add switches (choose **Configure > Switches**) and monitor switch operation (choose **Monitor > Switches**). Each switch counts as a single device against the total device count for your license. If you have unused device counts available in your license engine, you can add a switch to the NCS. If you have no remaining device counts available, you cannot add additional switches to the NCS.
- Switch Port Tracing (SPT) only switches—Switches perform switch port tracing only. SPT-only switches appear in the Configure > Switches page and in inventory reports, but SPT-only switches do not appear in the Monitor > Switches page or on the dashboards. Licensing does not apply to SPT switches.

Viewing Switches

Choose **Configure > Switches** to see a summary of all switches in the NCS database. The summary information includes the following:

- Management IP Address—IP address of the switch. Click the IP address of a switch to get more details. See the "Viewing Switch Details" section on page 8-201 for more information.
- Device Name—Name of the switch.
- Device Type—Type of switch.
- Reachability Status—Indicates Reachable if the switch is reachable or Unreachable if the switch is unreachable.
- Inventory Collection Status—Status of the last inventory collection. The possible values are OK, Partial, Failed, NA (for SPT-only switches), or In Progress.
- Inventory Status Detail—Specifies the status of the latest inventory collection. If the inventory collection was not successful, lists the possible reasons for the failure.
- Last Inventory Collection Date—Displays the most recent date in which the inventory was collected.
- Creation Time—Date and time the switch was added to the NCS.
- License Status—Indicates the license status of the switch, which can be Full Support or SPT only. See the "Features Available by Switch Type" section on page 8-200 for more information.

Click any column heading to sort the information by that column. You can switch between ascending and descending sort order by clicking the column heading more than once.

Viewing Switch Details

Choose **Configure > Switches** to see a summary of all switches in the NCS database. Click an IP address in the Management IP Address column to see detailed information about that switch Table 8-7 describes the summary information that is displayed.

Table 8-7 Configure > Switches Summary Information

General Parameters	
IP Address	IP address of the switch.
Device Name	Name of the switch.
Last Inventory Collection Date	Date and time of the last inventory collection.
Inventory Collection Status	Status of the last inventory collection. The possible values are OK, Partial, or Failed.
Software Version	Version of software running on the switch.
Location	Location of the switch.
Contact	Contact name for the switch.
Reachability Status	Indicates **Reachable** if the switch is reachable or **Unreachable** if the switch is unreachable.
SNMP Parameters	

Table 8-7 Configure > Switches Summary Information (continued)

General Parameters	
Version	SNMP version number, which can be v1, v2c, or v3. **Note** For switch port tracing to be successful in switches configured with SNMP v3, the context for the corresponding VLAN must be configured in the switch. See the "Configuring SNMPv3 on Switches" section on page 8-204 for more information.
Retries	Retries (in seconds) allowed before the process stops without success.
Timeout	SNMP timeout value (in seconds).
If you selected v3 in the Version drop-down list, the following fields appear:	
Username	Username
Auth. Type	Authentication type with can be None, HMAC-SHA, or HMAC-HD5.
Auth. Password	Authentication password.
Privacy Type	Privacy type with can be None, CBC-DES, or CFB-AES-128.
Privacy Password	Privacy password.
Community	If you selected v1 or v2c, this field indicates the SNMP community string.
Telnet/SSH Parameters	
Protocol	Protocol used.
User Name	Username.
Password	Password.
Confirm Password	Confirm the password by entering it again.
Enable Password	Enable password.
Confirm Password	Confirm the password by entering it again.
Timeout	Timeout value (in seconds).

Modifying SNMP Parameters

To modify SNMP parameters for a switch, follow these steps:

Step 1 Choose **Configure > Switches**, then click the IP address of the switch for which you want to change SNMP credentials.

Step 2 Modify the necessary SNMP Parameters fields, then click the following:

- **Reset** to restore the previously saved parameters.
- **Save** to save and apply the changes you made.
- **Cancel** to exit without saving your changes and return to the previous screen.

Modifying Telnet/SSH Parameters

To modify Telnet or SSH parameters for a switch, follow these steps:

Step 1 Choose **Configure > Switches**, then click the IP address of the switch for which you want to change Telnet or SSH credentials.

Step 2 Modify the necessary Telnet/SSH Parameters fields, then click the following:

- **Reset** to restore the previously saved parameters.
- **Save** to save and apply the changes you made.
- **Cancel** to exit without saving your changes and return to the previous screen.

Adding Switches

When you add a switch to the NCS database, by default, the NCS verifies the SNMP credentials of the switch. If the device credentials are not correct, you receive an SNMP failure message but the switch is added to the NCS database.

To add a switch to the NCS, follow these steps:

Step 1 Choose **Configure > Switches**.

Step 2 From the Select a command drop-down list, choose **Add Switches**, then click **Go**.

Step 3 Complete the fields as described in Table 8-8.

Table 8-8 Adding a Switch

Field	Description
General Parameters	
Add Format Type	Select: • **Device Info** to manually enter comma-separated IP addresses of Ethernet switches. • **CSV File** to import a CSV file that contains IP addresses of multiple switches. Enter the CSV file path in the text box or click **Browse** to navigate to the CSV file on your computer. See the "Configuring SNMPv3 on Switches" section on page 8-204 for more information.
IP Addresses	If you selected Device Info, enter comma-separated IP addresses of the Ethernet switches.
License Level	Select: • **Full** • **SPT only** to specify Switch Port Tracing support only.
SNMP Parameters **Note** Enter SNMP parameters for the write access, if available. If you enter read-only access parameters, the switch is added but the NCS is unable to modify the configuration.	
Version	Enter the SNMP version number, which can be v1, v2c, or v3. **Note** For switch port tracing to be successful in switches configured with SNMP v3, the context for the corresponding VLAN must be configured in the switch. See the "Configuring SNMPv3 on Switches" section on page 8-204 for more information.
Retries	Enter the retries (in seconds) allowed before the process stops without success.
SNMP Timeout (in secs)	Enter the SNMP timeout value (in seconds).

Table 8-8 Adding a Switch (continued)

Field	Description
If you selected v1 or v2c in the Version drop-down list, the Community field appears:	
Community	Enter the SNMP community string.
If you selected v3 in the Version drop-down list, the following fields appear:	
Username	Enter the username.
Auth. Type	Enter the authentication type with can be None, HMAC-SHA, or HMAC-HD5.
Auth. Password	Enter the authentication password.
Privacy Type	Enter the privacy type with can be None, CBC-DES, or CFB-AES-128.
Privacy Password	Enter the privacy password.
Telnet/SSH Parameters	
Protocol	Select the protocol.
User Name	Enter the username.
Password	Enter the password.
Confirm Password	Confirm the password by entering it again.
Enable Password	Enter the enable password.
Confirm Password	Confirm the enable password by entering it again.
Timeout (in secs)	Enter the timeout value (in seconds).

Step 4 Click **Add** to add the switch.

Step 5 Click **Cancel** to cancel the operation and return to the list of switches.

Note After adding a switch, it is placed temporarily in the Monitor > Unknown Devices page while the NCS attempts to communicate with the controller that you have added. Once communication with the switch has been successful, the switch moves from the Monitor > Unknown Devices page to the Monitor > Switches page. If the NCS is unable to successfully communicate with a switch, it remains in the Monitor > Unknown Devices and an error condition an error message is displayed. To access the Unknown Devices page, choose Configure > Unknown Devices.

Configuring SNMPv3 on Switches

The following is an example for configuring SNMPv3 on the switch:

```
snmp-server view v3default iso included
snmp-server group v3group v3 auth write v3default snmp-server user <username>
<v3group> v3 auth <md5 or sha> <authentication password>
```

If the switch has VLANs, you must configure each VLAN, otherwise switch porting tracing fails. The following is an example if the switch has VLANs 1 and 20.

```
snmp-server group v3group v3 auth context vlan-1  write v3default
snmp-server group v3group v3 auth context vlan-20 write v3default

snmp-server group v3group v3 auth context vlan-20 write v3default
```

Note When you create SNMP v3 view, make sure you include all of the OIDs.

Sample CSV File for Importing Switches

The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory. The following example shows a sample CSV file.

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name,
snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password,
snmp_retries,
snmp_timeout,protocol,telnet_username,telnet_password,enable_password,telnet_timeout
16.1.1.3,255.255.255.0,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
16.1.1.4,255.255.255.0,v2,public,,,,,3,10,ssh2,cisco,cisco,cisco,60
16.1.1.5,255.255.255.0,v2,public,,,,,3,10,,cisco,cisco,cisco,60
16.1.1.6,255.255.255.0,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
3.3.3.3,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4
4.4.4.4,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4,telnet,cisco,cisco,
cisco,60
```

The CSV file can contain the following fields:

- ip_address—IP address
- network_mask—Network mask
- snmp_version—SNMP credentials version. Can be v1, v2, or v3.
- snmp_community—SNMP community (Mandatory for v2.)
- snmpv2_community—SNMP V2 community.
- snmpv3_user_name—SNMP V3 username (Mandatory for v3.)
- snmpv3_auth_type—SNMP V3 authorization type. Can be None or HMAC-MD5 or HMAC-SHA (Mandatory for v3.)
- snmpv3_auth_password—SNMP V3 authorization password (Mandatory for v3).
- snmpv3_privacy_type—SNMP V3 privacy type. Can be None or DES or CFB-AES-128 (Mandatory for v3.)
- snmpv3_privacy_password—SNMP V3 privacy password (Mandatory for v3.)
- snmp_retries—SNMP retries
- snmp_timeout—SNMP timeout
- protocol—telnet, ssh2
- telnet_username—for switches and APs, if configured (Mandatory if configured.)
- telnet_password—for switches and APs (mandatory)
- enable_password
- telnet_timeout

Configuring Switch NMSP and Location

Choose **NCS > Configure > Switches >** *Switch IP Address* **> NMSP & Location** to view the NMSP and Location information for switches.

Note NMSP is supported by the following:

- Cisco Catalyst 3000 and 4000 series switches
- Cisco IOS Release 12.50 and later

You can enable or disable NMSP status and configure switch and switch port location as described in the following sections:

- Enabling and Disabling NMSP for Switches
- Configuring a Switch Location
- Configuring a Switch Port Location

Enabling and Disabling NMSP for Switches

You can enable or disable NMSP for a switch by choosing **NCS > Configure > Switches >** *Switch IP Address* **> NMSP & Location > NMSP Status**.

Table 8-9 lists the options available in the NMSP Status page.

Field	Description
NMSP	Select or Unselect this option to enable or disable NMSP for the switch.
MSE IP Address	Displays the IP address of the MSE if the switch is associated to an MSE. To associate this switch to an MSE, click **Go to Synchronize**. This takes you to the Synchronization page. You can synchronize this switch with an MSE. Alternately, you can choose **NCS > Services > Synchronize Services > Wired Switches** to synchronize switches to an MSE. For more information on Synchronization, see the "Synchronizing Services" section on page 11-11.

Configuring a Switch Location

You can configure the location for a switch using the Switch Location option.

Step 1 Choose **NCS > Configure > Switches >** *Switch IP Address* **> NMSP & Location > Switch Location**.

Step 2 In the Map Location pane, choose the following from the drop-down lists:

- **Campus**
- **Building**
- **Floor**

Step 3 Click **Import Civic** to import the civic information to the switch.

The fields in the Civic Location pane are populated after the civic information is imported.

Configuring a Switch Port Location

You can configure location for switch ports using the Switch Port Location option.

Step 1 Choose **NCS > Configure > Switches >** *Switch IP Address* **> NMSP & Location > Switch Port Location**.

Step 2 Select one or more ports on which you want to configure location.

Step 3 From the drop-down list, choose **Configure Location**, then click **Go**.

The Switch Port Location Configuration page appears.

The Switch Ports pane lists the ports that you have selected to configure location.

Step 4 In the Map Location pane, choose the following from the drop-down lists:

- **Campus**
- **Building**
- **Floor**

Step 5 Click **Import Civic** to import the civic information to the switch port.

The fields in the Civic Location pane are populated after the civic information is imported.

Removing Switches

When you remove a switch from the NCS database, the following functions are performed:

- Inventory information for that switch is removed from the database.
- Alarms for the switch remain in the database with a status of Clear. By default, cleared alarms are not displayed in the NCS interface.
- Saved reports remain in the database even if the switch on which the report was run is removed.

To remove a switch from the NCS, follow these steps:

Step 1 Choose **Configure > Switches**.

Step 2 Select the check box(es) of the switch(es) you want to remove.

Step 3 From the Select a command drop-down list, choose **Remove Switches**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Refreshing Switch Configuration

By default, inventory information is collected every six hours. If you make configuration changes and want the changes displayed immediately instead of waiting for the next inventory collection, you can refresh the switch as shown in the following steps:

Step 1 Choose **Configure > Switches**.

Step 2 Select the check box(es) of the switch(es) whose configuration you want to refresh.

Step 3 From the Select a command drop-down list, choose **Refresh Config from Switch**.

Step 4 Click **Go**.

Enabling Traps and Syslogs on Switches for Wired Client Discovery

This section describes how to configure switches to send traps and syslogs to the NCS to discover the clients as they connect/disconnect.

This section contains of the following topics:

MAC Notification for Traps (Used for Non-Identity Client Discovery)

This Cisco IOS switch feature forwards SNMP traps from the switch to the NCS server for MAC notifications (for non-802.1x clients).

Cisco IOS configuration example:

```
snmp-server enable traps mac-notification change move threshold
snmp-server host<IP address of NCS server> version 2c <community-string> mac-notification
mac address-table notification change interval 5
mac address-table notification change history-size 10
mac address-table notification change


interface <interface>
 description non-identity clients
 switchport access vlan <VLAN ID>
 switchport mode access
 snmp trap mac-notification change added  <- interface level config for MAC Notification
  snmp trap mac-notification change removed <- interface level config for MAC Notification
```

Debug Commands

```
debug snmp packets
```

Show Commands

```
show mac address-table notification change
```

References

For more information about configuring MAC Change Notification Traps, see the following URL: http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/swadmin.html#wp1246821

Syslog Configuration

Note This feature is used for identity clients discovery.

The syslog configuration forwards syslog messages from a Catalyst switch to the NCS server.

Cisco IOS configuration example:

```
archive
 log config
  notify syslog contenttype plaintext
logging facility auth
logging <IP address of NCS server>
```

For more information, see the following URL: http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_50_se/configuration/guide/swlog.html

Configuring Unknown Devices

To configure the unknown devices, follow these steps:

Step 1 Choose **Configure > Unknown Devices**. The Unknown Devices page appears. The summary information includes the following:

- IP Address—IP address of the device.
- Device Type—Type of device.
- Reachability Status—Indicates Reachable if the device is reachable or Unreachable if the device is unreachable.
- Inventory Collection Status—Status of the last inventory collection. The possible values are OK, Partial, Failed, NA, or In Progress.
- Inventory Status Detail—Specifies the status of the latest inventory collection. If the inventory collection was not successful, lists the possible reasons for the failure.
- Creation Time—Date and time the device was added to NCS.

Step 2 From the Unknown Devices page, you can perform the following functions:

- Remove Devices—To remove a device from the unknown devices table, select the device(s) and choose **Remove Devices** from the Select a command drop-down list.
- Update Device Credentials—To update the device credentials of a device, select the device and choose **Update Device Credentials** from the Select a command drop-down list. The Update Device Credentials page appears.

- Bulk Update Devices—To update the device credentials in a bulk, select **Bulk Update Devices** from the Select a command drop-down list. The Bulk Update Devices page appears. You can choose a CSV file.

Note The CSV file contains a list of devices to be updated, one device per line. Each line is a comma separated list of device attributes. The first line describes the attributes included. The IP address attribute is mandatory.

Configuring Spectrum Experts

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to the NCS. This feature allows the NCS to collect, monitor, and archive detailed interferer data from Spectrum Experts in the network.

To configure spectrum experts, choose **Configure > Spectrum Experts**. This page provides a list of all Spectrum Experts including:

- Hostname—The hostname or IP address of the Spectrum Expert laptop.
- MAC Address—The MAC address of the spectrum sensor card in the laptop.
- Reachability Status—Specifies whether the Spectrum Expert is successfully running and sending information to the NCS. The status appears as reachable or unreachable.

This section contains the following topics:

- Adding a Spectrum Expert, page 8-210
- Monitoring Spectrum Experts, page 8-211

Adding a Spectrum Expert

To add a Spectrum Expert, follow these steps:

Step 1 Choose **Configure > Spectrum Experts**.

Step 2 From the Select a command drop-down list, choose **Add Spectrum Expert**.

Note This link only appears when no spectrum experts are added. You can also access the Add Spectrum Expert page by choosing **Add Spectrum Expert** from the Select a command drop-down list.

Step 3 Enter the hostname or IP address of the Spectrum Expert. If you use hostname, your spectrum expert must be registered with DNS to be added to the NCS.

Note To be correctly added as a spectrum expert, the spectrum expert client must be running and configured to communicate to the NCS.

Monitoring Spectrum Experts

You also have the option to monitor spectrum experts.

To monitor spectrum expert, follow these steps:

Step 1 Choose **Monitor > Spectrum Experts**.

Step 2 From the left sidebar menu, you can access the Spectrum Experts page and the Interferers-SEs page.

Viewing Spectrum Experts Summary

The Spectrum Experts page provides a table of the Spectrum Experts added to the system. The table provides the following Spectrum Expert information:

Hostname—Displays the host name or IP address.

Active Interferers—Indicates the current number of interferes being detected by the Spectrum Experts.

Alarms APs—The number of access points seen by the Spectrum Experts that are potentially affected by detected interferers.

Alarms—The number of active interference traps sent by the Spectrum Expert. Click to access the Alarm page that is filtered to the active alarms for this Spectrum Expert.

Reachability Status—Indicates “Reachable” in green if the Spectrum Expert is running and sending data to the NCS. Otherwise, indicates “unreachable” in red.

Location—When the Spectrum Expert is a wireless client, a link for location is available. It shows the location of the Spectrum Expert with a red box that shows the effective range.

Viewing Interferers Summary

The Interferers-SEs page displays a list of all the interferers detected over a 30-day interval. The table provides the following interferer information:

- Interferer ID—An identifier that is unique across different spectrum experts. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, which you can use to find the interfering device.
- Category—Indicates the category of the interferer. Categories include: Bluetooth, cordless phones, microwave ovens, 802.11 FH, generic: fixed-frequency, jammers, generic: frequency-hopped, generic:continuous, and analog video.
- Type—Active indicates that the interferer is currently being detected by a spectrum expert. Inactive indicates that the interferer is no longer detected by a spectrum expert or the spectrum expert saw that the interferer is no longer reachable by the NCS.
- Discover Time—Indicates when the interferer was discovered.

- Affected Channels—Identifies affected channels.
- Number of APs Affected—The number of access points managed by the NCS that the spectrum expert detects or the interferers that the spectrum expert detected on the channels of the access point. Only active interferers are shown. If all of the following conditions are met, the access point is labelled as *affected*:
  - If the access point is managed by the NCS.
  - If the spectrum expects detects the access point.
  - If the spectrum expert detects an interferer on the serving channel of the access point.
- Power—Indicated in dBm.
- Duty Cycle—Indicated in percentage. 100% is the worst value.
- Severity—Indicates the severity ranking of the interferer. 100 is the worst case whereas 0 is no interference.

Viewing Spectrum Experts Details

The Spectrum Expert page provides all interference details from a single Spectrum Expert. This page updates every 20 seconds and gives a real-time look at the remote spectrum expert. This page includes the following items:

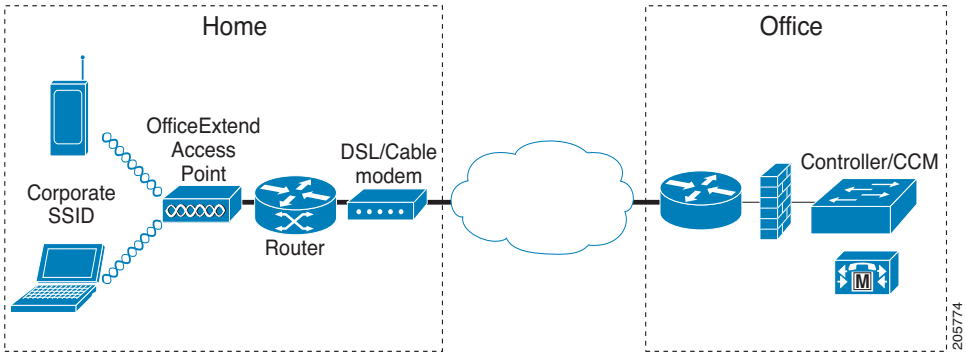
- Total Interferer Count—Given from the specific spectrum expert.
- Active Interferers Count Chart—Displays a pie chart that groups interferers by category.
- Active Interferer Count Per Channel—Displays the number of interferers grouped by category on different channels.
- AP List—Provides a list of access points detected by the spectrum expert. These access points are on channels that have active interferers detected.
- Affected Clients List—Provides a list of clients that are currently authenticated to an access point. You can select specific RADIUS or LDAP servers to provide external authentication in the Security > AAA page.

OfficeExtend Access Point

An OfficeExtend access point provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to the residence of an employee. The experience of a teleworker at the home office is exactly the same as it is at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Figure 8-23 illustrates a typical OfficeExtend access point setup.

Figure 8-23 Typical OfficeExtend Access Point Setup



Note OfficeExtend access points are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), thereby enabling an entire group of computers to be represented by a single IP address. In controller release 6.0, only one OfficeExtend access point can be deployed behind a single NAT device.

Currently, only Cisco Aironet 1130 series and 1140 series access points that are joined to a Cisco 5500 series controller with a WPlus license can be configured to operate as OfficeExtend access points.

Note Your firewall must be configured to allow traffic from access points using CAPWAP. Make sure that UDP ports 5246 and 5247 are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.

Licensing for an OfficeExtend Access Point

Make sure that the WPlus license is installed on the 5500 series controller. After the license is installed, you can enable the OfficeExtend mode on an 1130 series or 1140 series access point.

Note The operating system software automatically detects and adds an access point to the NCS database as it associates with existing controllers in the NCS database.

Configuring Link Latency Settings for Access Points

You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to a controller but is especially useful for FlexConnect access points, for which the link could be a slow or unreliable WAN connection.

Note Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the access point to the controller and back. This time can vary due to network link speed and controller processing loads. The access point timestamps the outgoing echo requests to the controller and the echo requests received from the controller. The access point sends this delta time to the controller as the system round-trip time. The access point sends heartbeat packets to the controller at a default interval of 30 seconds.

Note Link latency calculates the CAPWAP response time between the access point and the controller. It does not measure network latency or ping responses.

The controller displays the current round-trip time as well as a running minimum and maximum round-trip time. The minimum and maximum times continue to run as long as the controller is up or can be cleared and allowed to restart.

To configure link latency, follow these steps:

Step 1 In the Configure > Access Point details page, select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. The default value is unselected.

Step 2 Click **Save** to save your changes.

The link latency results appear below the Enable Link Latency check box:

- Current—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- Minimum—Because link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- Maximum—Because the link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

Step 3 To clear the current, minimum, and maximum link latency statistics on the controller for this access point, click **Reset Link Latency**. The updated statistics appear in the Minimum and Maximum fields.

Configuring Chokepoints

Chokepoints are low frequency transmitting devices. When a tag passes within range of placed chokepoint, the low-frequency field awakens the tag that in turn sends a message over the Cisco Unified Wireless Network including the chokepoint device ID. The transmitted message includes sensor information (such as temperature and pressure). A chokepoint location system provides room level accuracy (ranging from few inches to 2 feet depending on the vendor).

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be entered into the location database and plotted on a NCS map.

This section contains the following topics:

Configuring New Chokepoints

This section contains the following topics:

Adding a Chokepoint to the NCS Database

To add a chokepoint to the NCS database, follow these steps:

Step 1 Choose **Configure > Chokepoints**.

Step 2 From the Select a command drop-down list, choose **Add Chokepoints**.

Step 3 Click **Go**.

Step 4 Enter the MAC address and name for the chokepoint.

Step 5 Select the check box to indicate that it is an Entry/Exit Chokepoint.

Step 6 Enter the coverage range for the chokepoint.

Note Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 7 Click **OK**.

Note After the chokepoint is added to the database, it can be placed on the appropriate NCS floor map.

Adding a Chokepoint to an NCS Map

To add the chokepoint to a map, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 In the Maps page, click the link that corresponds to the floor location of the chokepoint.

Step 3 From the Select a command drop-down list, choose **Add Chokepoints**.

Step 4 Click **Go**.

Note The Add Chokepoints summary page lists all recently-added chokepoints that are in the database but not yet mapped.

Step 5 Select the check box next to the chokepoint that you want to place on the map.

Step 6 Click **OK**.

A map appears with a chokepoint icon located in the top-left hand corner. You are now ready to place the chokepoint on the map.

Step 7 Left-click the chokepoint icon and drag and place it in the proper location.

Note The MAC address, name, and coverage range of the chokepoint appear in the selected chokepoints detail page when you click the chokepoint icon for placement.

Step 8 Click **Save**.

You are returned to the floor map and the added chokepoint appears on the map.

Note The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.

Note The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

Note MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint display when you pass a mouse over its map icon

Step 9 If the chokepoint does not appear on the map, select the **Chokepoints** check box located in the Floor Settings menu.

Note Do not select the **Save Settings** check box unless you want to save this display criteria for all maps.

Note You must synchronize network design to the mobility services engine or location server to push chokepoint information.

Removing a Chokepoint from an NCS Map

To remove an chokepoint from the map, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 In the Maps page, choose the link that corresponds to the floor location of the chokepoint.

Step 3 From the Select a command drop-down list, choose **Remove Chokepoints**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Removing a Chokepoint from the NCS

To remove an chokepoint from the NCS, follow these steps:

Step 1 Choose **Configure > Chokepoints**.

Step 2 Select the check box of the chokepoint that you want to delete.

Step 3 From the Select a command drop-down list, choose **Remove Chokepoints**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Editing Current Chokepoints

To edit a current chokepoint in the NCS database and appropriate map, follow these steps:

Step 1 Choose **Configure > Chokepoints**. The Configure > Chokepoints page displays the following information for each current chokepoint: MAC address, chokepoint name, entry/exit chokepoint, range, static IP address, and map location for the chokepoint.

Step 2 Click the chokepoint you want to edit in the MAC Address column.

Step 3 Edit the following parameters, as necessary:

- Name
- Entry/Exit Chokepoint—Click to enable.
- Range—Coverage range for the chokepoint.

Note The chokepoint range is product-specific and is supplied by the chokepoint vendor.

- Static IP Address

Step 4 Click **Save**.

Configuring Wi-Fi TDOA Receivers

This section contains the following topics:

Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting

The Wi-Fi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine to aid in the location calculation of the asset. TDOA receivers use the method of Time Difference of Arrival (TDOA) to calculate tag location. This method uses data from a minimum of three TDOA receivers to generate a tagged asset location.

Note

- If a TDOA receiver is not in use and the partner engine software is resident on the mobility service engine, then the location calculations for tags are generated using RSSI readings from access points.
- The Cisco Tag engine can calculate the tag location using the RSSI readings from access points.

Before using a TDOA receiver within the Cisco Unified Wireless Network, you must perform the following steps:

1. Have a mobility services engine active in the network.

   See the "Adding a Mobility Services Engine" section on page 11-6 for details on adding a mobility services engine.

2. Add the TDOA receiver to the NCS database and map.

   See the "Adding Wi-Fi TDOA Receivers to the NCS and Maps" section on page 8-218 for details on adding the TDOA receiver to the NCS.

3. Activate or start the partner engine service on the MSE using the NCS.
4. Synchronize the NCS and mobility services engines.

   See the "Synchronizing Services" section on page 11-11 for details on synchronization.

5. Set up the TDOA receiver using the AeroScout System Manager.

Note See the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide* for configuration details at the following URL: http://support.aeroscout.com.

Adding Wi-Fi TDOA Receivers to the NCS and Maps

After the Wi-Fi TDOA receiver is installed and configured by the AeroScout System Manager and the partner software is downloaded on the mobility services engine, you are ready to add the TDOA receiver to the mobility services engine database and position it on an NCS map.

After adding TDOA receivers to the NCS maps, you continue to make configuration changes to the TDOA receivers using the AeroScout System Manager application rather than the NCS.

Note For more details on configuration options, see the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide* at the following URL: http://support.aeroscout.com.

To add a TDOA receiver to the NCS database and appropriate map, follow these steps:

Step 1 Choose **Configure > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

Note To view or edit current WiFi TDOA receiver details, click the MAC Address link to open the details page.

Step 2 From the Select a command drop-down list, choose **Add WiFi TDOA Receivers**.

Step 3 Click **Go**.

Step 4 Enter the MAC address, name and static IP address of the TDOA receiver.

Step 5 Click **OK** to save the TDOA receiver entry to the database.

Note After you add the TDOA receiver to the database, you can place the TDOA receiver on the appropriate NCS floor map. To do so, continue with Step 6.

Note A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Step 6 To add the TDOA receiver to a map, choose **Monitor > Maps**.

Step 7 In the Maps page, select the link that corresponds to the floor location of the TDOA receiver.

Step 8 From the Select a command drop-down list, choose **Add WiFi TDOA receivers**.

Step 9 Click **Go**.

Note The All WiFi TDOA Receivers summary page lists all recently-added TDOA receivers that are in the database but not yet mapped.

Step 10 Select the check box next to each TDOA receiver to add it to the map.

Step 11 Click **OK**. A map appears with a TDOA receiver icon located in the top-left hand corner. You are now ready to place the TDOA receiver on the map.

Step 12 Left-click the TDOA receiver icon and drag and place it in the proper location on the floor map.

Note The MAC address and name of the TDOA receiver appear in the left pane when you click the TDOA receiver icon for placement.

Step 13 Click **Save** when the icon is placed correctly on the map. The added TDOA receiver appears on the floor heat map.

Note The icon for the newly added TDOA receiver might or might not appear on the map depending on the display settings for that floor. If the icon did not appear, proceed with Step 14.

Step 14 If the TDOA receiver does not appear on the map, click **Layers** to collapse a selection menu of possible elements to display on the map.

Step 15 Select the **WiFi TDOA Receivers** check box. The TDOA receiver appears on the map.

Note When you place your cursor over a TDOA receiver on a map, configuration details display for that receiver.

Step 16 Click **X** to close the Layers page.

Note Do not choose **Save Settings** from the Layers menu unless you want to save this display criteria for all maps.

Step 17 You can now download the partner engine software to the mobility services engine.

Viewing or Editing Current Wi-Fi TDOA Receivers

To view a current TDOA receiver to the NCS database, follow these steps:

Step 1 Choose **Configure > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

Step 2 Click the MAC Address link to view the TDOA receiver details including MAC address, name, and static IP address.

Step 3 If you make any changes to the receiver name or IP address, click **Save** to confirm these changes.

Note A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Removing Wi-Fi TDOA Receivers from NCS and Maps

You can remove one or multiple WiFi TDOA receivers at a time. If you remove a TDOA receiver from a map it remains in the NCS database but is labeled as unassigned.

To delete a TDOA receiver from the NCS, follow these steps:

Step 1 Choose **Configure > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

Step 2 Select the check box next to each TDOA receiver to be deleted.

Step 3 From the Select a command drop-down list, choose **Remove WiFi TDOA Receivers**.

Step 4 Click **Go**.

Step 5 To confirm TDOA receiver deletion, click **OK** in the dialog box.

In the **All WiFi TDOA Receivers** page, a message confirms the deletion. The deleted TDOA receiver is no longer listed in the page.

Configuring Scheduled Configuration Tasks

The Scheduled Configuration Tasks feature allows you to view, modify, and delete scheduled access point template and configuration group tasks. To access the Scheduled Configuration Tasks page, choose **Configure > Scheduled Configuration Tasks**.

This section contains the following topics:

AP Template Tasks

The AP Template Tasks page allows you to view, modify, delete, enable, or disable current access point template tasks. To access the AP Template Tasks page and view current access point template tasks, choose **Configure > Scheduled Configuration Tasks**.

Modifying a Current AP Template Task

To modify a current access point template task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Select the template name of the applicable task.

Step 3 In the AP Radio/Template page, click the **Apply/Schedule** tab.

Step 4 Make any necessary changes to the current schedule or access point template, and click **Schedule**.

Viewing AP Status Report for the Scheduled Task

The AP Status Report for the scheduled task includes the following information:

- AP Name—Lists all of the access points included in the scheduled access point template task.
- Ethernet MAC—Indicates the Ethernet MAC addresses for the applicable access points.
- Controller—Indicates the associated controller for each of the applicable access points.
- Map—Displays the map location for the applicable access points.
- Status—Indicates whether the access point template has been successfully applied. Possible states include Not Initiated, Success, Failure, Partial Failure, and Not Reachable.

- Task Execution Time—Indicates the execution time of the scheduled task for the applicable access point.

To view the status report for the access points included in the scheduled task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Select the AP Status Report for the applicable task.

Enabling or Disabling a Current AP Template Task

To enable or disable a current access point template task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Select the check box of the scheduled task to be enabled or disabled.

Step 3 From the Select a command drop-down list, choose **Enable Schedule** or **Disable Schedule**, as applicable.

Step 4 Click **Go**.

Viewing AP Template Task History

To view previous scheduled task reports, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Select the check box of the applicable scheduled task.

Step 3 From the Select a command drop-down list, choose **View History**.

Step 4 Click **Go**.

Deleting a Current AP Template Task

To delete a scheduled access point template task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Select the check box of the applicable scheduled task.

Step 3 From the Select a command drop-down list, choose **Delete Task(s)**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Configuring Config Groups

The Config Group Tasks page allows you to view, modify, delete, enable, or disable current configuration group tasks. To access the Config Group Tasks page and view current config group tasks, choose **Configure > Scheduled Configuration Tasks > ConfigGroup**.

Modifying a Current Config Group Task

To modify a current configuration group task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Select the group name of the applicable task.

Step 4 From the Config Groups page, click the **Apply/Schedule** tab.

Step 5 Make any necessary changes to the current schedule, and click **Schedule**.

Viewing Controller Status Report for the Scheduled Task

The Controller Status Report for the scheduled task includes the following information:

- Group Name—Name of the config group.
- Schedule—Indicates whether the task is enabled, disabled, or expired.
- Last Run Time—Indicates the date and time of the most recent scheduled task.
- Next Scheduled Run—Indicates the date and time of the next scheduled task.
- Controller Status Report—Indicates the number of status reports for this config group. Click the number link to view the status reports.

To view the controller status report, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Select the Controller Status Report for the applicable task. The Controller Status Report provides the following information:

- Controller
- Status of task (such as Not Initiated, Success, Failure, Partial Failure, Partial Success, Not Reachable)
- Number of templates applied

- Number of templates failed
- Time and date of the task execution

Enabling or Disabling a Current Config Group Task

To enable or disable a current configuration group task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Select the check box of the scheduled task to be enabled or disabled.

Step 4 From the Select a command drop-down list, choose **Enable Schedule** or **Disable Schedule**, as applicable.

Step 5 Click **Go**.

Viewing Config Group Task History

To view previous scheduled task reports, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Select the check box of the applicable scheduled task.

Step 4 From the Select a command drop-down list, choose **View History**.

Step 5 Click **Go**.

Deleting a Current Config Group Task

To delete a scheduled configuration group task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Select the check box of the applicable scheduled task.

Step 4 From the Select a command drop-down list, choose **Delete Task(s)**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion.

Viewing WLAN Configuration Scheduled Task Results

Note There is no drop-down command list provided for WLAN Configuration.

To view and manage all scheduled WLAN tasks in the NCS, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **WLAN Configuration** to open the WLAN Configuration Task List page.

Step 3 If scheduled configuration tasks are available, the WLAN Configuration Task List page contains the following parameters:

- Schedule Task Name—The user-defined name of the new scheduled task.
- Schedule—Indicates the status of the scheduled task.
- WLAN Status—Indicates the status of the WLAN.
- Controller IP Address—Indicates the IP address of the controller.
- Last Run Time—Indicates the date and time of the most recent scheduled task.
- Next Scheduled Run—Indicates the date and time of the next scheduled task.
- Recurrence—Indicates Daily or Weekly if the scheduled task is recurring.

Step 4 Select the Task Name link to open the WLAN Schedule Detail page. In this page, you can modify the date and time of the scheduled task. See the "Managing WLAN Status Schedules" section on page 8-77 for more information.

Step 5 Select the check box of the scheduled task and use the Select a command drop-down list located in the WLAN Configuration Task List page to enable, disable, or delete selected tasks.

- Enable Schedule—Enable the task if its schedule is disabled on the server.
- Disable Schedule—Disable the running scheduled task on the server. Once disabled, the task does not run at the scheduled time. You can re-enable the task at a later time.
- View History—View the execution results for individual WLAN tasks including reasons for any failures.
- Delete Task(s)—Delete the selected task from the NCS server.

Downloading Software Task

By using this feature you can schedule tasks for downloading software to controllers. The Download Software Tasks page allows you to add, delete, view, enable, or disable scheduled download software tasks. To access the Download Software Tasks page and view current download software tasks, choose **Configure > Scheduled Configuration Tasks > Download Software**.

This section contains the following topics:

Adding a Download Software Task

To add a download software task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software** to open the Download Software Task List page.

Step 3 From the Select a command drop-down list, choose **Add Download Software Task**.

Step 4 Click **Go**. The New Download Software Task page appears.

Step 5 Configure the following information:

- General
  - Task Name—Enter a Scheduled Task Name to identify this scheduled software download task.
- Schedule Details
  - Download Type—Select the download type. Select the **Download software to controller** check box to schedule download software to controller or select the **Pre-download software APs** check box to schedule the pre-download software APs. If you select Download software to controller, specify the image details.

Note The pre-download option is displayed only when all selected controllers are using the Release 7.0.x.x or later.

Note To see Image Predownload status per AP, enable the task in the Administration > Background Task > AP Image Predownload Task page, and run an AP Image Predownload report from the Report Launch Pad.

  - Reboot Type—Indicates whether the reboot type is manual, automatic, or scheduled.

Note Reboot Type Automatic can be set only when the **Download software to controller** option is selected.

  - Download date/time—Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date. Select the time from the hours and minutes drop-down lists.
  - Reboot date/time—This option appears only if select the reboot type “Scheduled”. Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date to reboot the controller. Choose the time from the hours and minutes drop-down lists.

Note Schedule enough time (at least 30mins) between Download and Reboot so that all APs can complete the software pre-download.

Note If any one of the AP is in pre-download progress state at the time of scheduled reboot, the controller does not reboot. In such a case, wait for the pre-download to finish for all the APs and reboot the controller manually.

- Notification (Optional)—Enter the e-mail address of recipient to send notifications via e-mail.

  Note To receive e-mail notifications, configure the NCS mail server in the Administration > Settings > Mail Server Configuration page.

- Image Details—Specify the TFTP or FTP Server Information:

  Note Complete these details if you selected the Download software to controller option in Schedule Details group box.

  TFTP—Specify the TFTP Server Information:

  - From the File is Located on drop-down list, choose **Local machine** or **TFTP server**.

    Note If you choose TFTP server, choose **Default Server** or **add a New server** from the Server Name drop-down list.

  - Specify the IP address of the TFTP server. This is automatically populated if the default server is selected.
  - Specify the local filename or click **Browse** to navigate to the appropriate file.
  - If you selected TFTP server previously, specify the filename.

  FTP—Specify the FTP Server Information:

  - FTP Credentials Information—Enter the FTP username, password, and port if you selected the FTP radio button.
  - From the File is Located on drop-down list, choose **Local machine** or **FTP server**.

    Note If you choose FTP server, choose **Default Server** or **add a New server** from the Server Name drop-down list.

  - Specify the IP address of the FTP server. This is automatically populated if the default server is selected.
  - Specify the local filename, or click **Browse** to navigate to the appropriate file.
  - If you selected FTP server previously, specify the filename.

Step 6 Click **Save**.

Modifying a Download Software Task

To modify a download software task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Select the Task Name link to open the Download Software Task page.

Step 4 Make any necessary changes.

Note Any changes in Download Type (Download/Pre-download) or Server Type (FTP/TFTP) for the task in 'Enabled' state sets the task to 'Disabled' state and all the existing controllers are disassociated from the task.

Step 5 Click **Save**.

Selecting Controllers for the Download Software Task

This page lists all the supported controllers that can be selected for the scheduled image download/pre-download task.

To select a controller for scheduled image download, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Click the Controller to open the Download Software Task details page.

Step 4 In the Download Software Task details page, Click **Select Controller** to view the controller list.

Note The Select Controllers page can also be accessed from Configure > Scheduled Configuration Tasks > Download Software > click hyperlink in the Select Controller column for any download task which is in Enabled, Disabled or in Expired state.

Note If the pre-download option is chosen for the task, then only the controllers with software Release 7.0.x.x or later are listed.

Note Controllers with Reachability Status 'Unreachable' cannot be selected for Download Software Task.

Step 5 Make any necessary changes.

Step 6 Click **Save**.

Viewing Download Software Results

To view the Schedule Run Results report, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Select the **Task Name** check box.

Step 4 From the Select a command drop-down list, choose **Schedule Run Results**.

Step 5 Click **Go**. The Schedule Run Results page provides the information:

- IP Address—The IP address of the controller to which the software to be downloaded.
- Controller Name—Name of the controller.
- Scheduled Run Time—Scheduled time of the download process.
- Last Updated Time—Last update time of the schedule download status (or result).
- Transfer Status—Current download status of the image in controller. For example, Not Initiated, Wrong file Type, Writing the code into flash, Transfer Successful.
- Reboot Status—Reboot status of the controller. For example, NA (if the reboot type is "Manual"), Reboot failed, Reboot Successful.
- Details—Detailed status about the download and reboot process.

Deleting a Download Software Task

To delete a scheduled download software task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Select the check box of the applicable scheduled task.

Step 4 From the Select a command drop-down list, choose **Delete Download Software Task**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion.

Enabling or Disabling a Download Software Task

To enable or disable a download software task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Select the check box of the scheduled task to be enabled or disabled.

Step 4 From the Select a command drop-down list, choose **Enable Schedule** or **Disable Schedule**, as applicable.

Step 5 Click **Go**.

Configuring Auto Provisioning for Controllers

Auto provisioning allows the NCS to automatically configure a new or replace a current wireless LAN controller (WLC). The NCS auto provisioning feature can simplify deployments for customers with a large number of controllers.

Note For Auto Provisioning privileges, you must have Admin, Root, or SuperUser status.

Note To allow or disallow a user Auto Provisioning privileges, edit the permitted tasks using Administration > AAA > User Groups > *group name* > List of Tasks Permitted in the NCS. Select or unselect the check box to allow or disallow these privileges.

Note A controller radio and b/g networks are initially disabled by the NCS downloaded startup configuration file. If desired, you might turn on those radio networks by using a template, which should be included as one of the automated templates.

Note To specify the Auto Provision filter contents, you can directly enter the details in the application or import the details from a CSV file. The auto provisioning feature supports the 5500 and non-5500 series controllers. The non-5500 series controllers have AP manager interface configuration information defined, whereas 5500 series controllers do not have this information.

To access the Auto Provisioning feature, choose **Configure > Controller Auto Provisioning**.

- Auto Provisioning Device Management (Auto Provisioning Filter List)—Allows you to create and edit auto provisioning filters which define the list of allowable devices to be auto provisioned or auto monitored by the NCS.
- Auto Provisioning Primary Search Key Settings—Provides the ability to set the matching criteria search order.

Auto Provisioning Device Management (Auto Provisioning Filter List)

This feature allows you to create and edit auto provisioning filters which define the list of allowable devices to be auto provisioned or auto monitored by the NCS.

Filter parameters include the following:

- Filter Name—Identifies the name of the filter.
- Filter Enable—Indicates whether or not the filter is enabled.

  Note Only enabled filters can participate in the Auto Provisioning process.

- Monitor Only—If selected, the WLC defined in this filter is managed by the NCS but not configured by the NCS if the WLC contacts the NCS during the auto provisioning process.
- Filter Mode—Indicates the search mode for this filter (Host Name, MAC Address, or Serial Number).

- Config Group Name—Indicates the Configuration Group name.

Note All Config-Groups used by auto provision filters should not have any controller defined in them.

Auto Provisioning Options

The Select a command drop-down list has the following options:

- Add Filter—Allows you to add an Auto Provisioning filter. See the "Adding an Auto Provisioning Filter" section on page 8-231 for more information.
- Delete Filter(s)—Allows you to delete the selected Auto Provisioning filter. See the "Deleting an Auto Provisioning Filter(s)" section on page 8-234 for more information.
- List Filter(s) Device Info—Allows you to view details for the selected Auto Provisioning filter. See the "Listing Auto Provisioning Filter(s) Device Information" section on page 8-235 for more information.
- List All Filter(s) Device Info—Allows you to view details for all of the Auto Provisioning filter. See the "Listing All Auto Provisioning Filter(s) Device Information" section on page 8-235 for more information.
- Export Filter(s) Config (CSV)—Allows you to export details for the selected Auto Provisioning filter. See the "Exporting Auto Provisioning Filter(s)" section on page 8-236 for more information.
- Export All Filter(s) Config (CSV)—Allows you to export details for all of the Auto Provisioning filter. See the "Exporting All Auto Provisioning Filter(s)" section on page 8-236 for more information.

This section contains the following topics:

Adding an Auto Provisioning Filter

To add an Auto Provisioning Filter, follow these steps:

Step 1 Choose **Configure > Controller Auto Provisioning**. The Auto Provisioning Filter List page appears

Step 2 From the Select a command drop-down list, choose **Add Filter**.

Step 3 Click **Go**.

Step 4 Click **Go**. The Auto Provisioning Filters > New Filter page appears.

Step 5 Configure the following information:

- General

  - Enable Filter—Select the check box to enable the new filter.

Note Only enabled filters can participate in the Auto Provisioning process.

  - Filter Name—Enter a filter name.

- Filter Properties
  - Monitor Only—If selected, the WLC defined in this Filter is managed by the NCS but not configured by the NCS if the WLC contacts the NCS during the auto provisioning process.
  - Filter Mode—From the drop-down list, choose **Host Name**, **MAC Address**, **Serial Number** to indicate the search mode for this filter.
  - Config Group Name—From the drop-down list, choose a config group name.
- Filter Member Management - Add Member
  - Input Type—From the drop-down list, choose **Single Device** or **CSV File**.

    If Single Device is selected, enter the host name, enable LAG configuration (if applicable), and enter the following: management interface IP Address, management interface netmask, management interface gateway, AP manager interface IP address, AP manager interface netmask, AP manager interface gateway, and DHCP IP address.

    If CSV File is selected, enter the CSV file or use the **Browse** button to navigate to the applicable CSV File.

Note You can choose the **Download a sample CSV File** link to download a sample CSV file to your computer and customize the various configurations.

Note Because MS-Excel can insert additional commas when you edit a CSV file, ensure that you edit the CSV file using a normal text editor application.

A CSV file contains the following sections:

** The first part is the General Config section that contains parameters which are used to construct controller's startup config file.
** The first line in the CSV file must be keyword

"!!deviceId, LAG, managementIP, managementVlanId, managementNetmask, managementGateway, apManagerIP, apManagerVlanId, apManagerNetmask, apManagerGateway, dhcpServerIP"

deviceId—it can be Host name, Mac address, or Serial number.
LAG—controller's LAG configuration (true/false).
managementIP—controller's Management interface IP address.
managementVlanId—controller's Management interface VLAN Id (0=untagged).
managementNetmask—controller's Management interface Network mask.
managementGateway—controller's Management interface Gateway IP.
apManagerIP—controller's AP Manager Interface IP address, optional for 5500 series controller.
apManagerVlanId—controller's AP Manager Interface VLAN Id (0=untagged), optional for 5500 series controller.

apManagerNetmask—controller's AP Manager Interface Netmask, optional for 5500 series controller.
apManagerGateway—controller's AP Manager Interface Gateway, optional for 5500 series controller.
dhcpServerIP—controller's DHCP IP address.

** The second part is the Dynamic Interface section that contains dynamic interface parameters for a controller. This is an optional section.
** To configure a dynamic interface, the first eight parameters are mandatory and the last four parameters are optional.

"!!deviceId, interfaceName, vlanId, quarantineVlanId, interfaceIP, interfaceNetmask, gateway, primaryPort, secondaryPort, primaryDHCP, secondaryDHCP, aclName"
deviceId—this deviceId must be defined previously in section 1.
interfaceName—name of the dynamic interface.
vlanId—vlan ID used by this interface.
quarantineVlanId—quarantine vlan ID used by this interface.
interfaceIP—IP address of the dynamic interface.
interfaceNetmask—Network Mask of the dynamic interface.
gateway—Gateway IP address of the dynamic interface.
primaryPort—physical primary port number used by the dynamic interface.
secondaryPort—physical secondary port number used by the dynamic interface, this is an optional field.
primaryDHCP—the IP address of the primary DHCP used by the dynamic interface, this is an optional field.
secondaryDHCP—IP address of the secondary DHCP used by the dynamic interface, this is an optional field.

** The third part is the Device Specific Config section, contains other device specific configuration parameters which are optional during auto provisioning.

"!!deviceId, countryCode, mobilityGroupName, mobilityGroupMembers"
deviceId—this deviceId must be defined previously in section 1.
countryCode—country code for the controller, this is an optional field.
mobilityGroupName—default name of the mobility group this controller belongs to, this is an optional field. If this attribute is not specified then the existing default mobility group name is used.
mobilityGroupMembers—IP addresses, Mac Addresses and mobility group name of the mobility group members of the controller, which are separated by semi colon, this is an optional field. Both IP address and Mac Address are required for a mobility group member, they are separated by forward slash. Mobility group name is an optional attribute in this field. If mobility group name is not present then the default mobility group name for this controller is used.

- If you select the Single Device option, configure the following options:
  - Device Type—From the drop-down list, choose **5500 Controller** or **non-5500 Controller**.
  - Host Name
  - LAG Configuration: Enabled or Disabled.
  - Management Interface IP Address
  - Management Interface VLAN Id (0=untagged)
  - Management Interface Netmask
  - Management Interface Gateway

- AP Manager Interface IP Address
- AP Manager Interface VLAN Id (0=untagged)
- AP Manager Interface Netmask
- AP Manager Interface Gateway
- DHCP IP Address—When the controller comes up after a reset, it uses this IP address to get a DHCP address, and identifies its TFTP server from where the configuration file needs to be picked.
- Virtual IP Address—An address which is not routable and usually configured as 209.105.170.1, as a DHCP server at the virtual IP address to wireless clients.

Step 6 Click **Submit**.

Note You can specify the Dynamic Interface configuration and Device Specific configuration details only when you input a CSV file. These two configurations cannot be performed using the graphical user interface.

Editing an Auto Provisioning Filter

To edit a Auto Provisioning filter, follow these steps:

Step 1 Choose **Configure > Controller Auto Provisioning**.

Step 2 Select the Filter Name of the filter you want to edit.

Step 3 Make the necessary changes to the current filter parameters.

Note To view detailed information for a filter member, select the Device ID check box of the member you want to view.
To delete a filter member. select the check box for the member you want to delete in the Filter Member Management - Delete Member group box. When you click Submit, that member is deleted.

Step 4 Click **Submit**.

Deleting an Auto Provisioning Filter(s)

To delete an Auto Provisioning Filter, follow these steps:

Step 1 Choose **Configure > Controller Auto Provisioning**.

Step 2 Select the check box of the filter you want to delete.

Step 3 From the Select a command drop-down list, choose **Delete Filter(s)**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Listing Auto Provisioning Filter(s) Device Information

To view details for an individual Auto Provisioning Filter, follow these steps:

Step 1 Choose **Configure > Controller Auto Provisioning**.

Step 2 Select the check box of the filter you want to view.

Step 3 From the Select a command drop-down list, choose **List Filter(s) Device Info**.

Step 4 Click **Go**. The Detailed Auto Provisioning Device Information page appears.

The following information is provided for the selected filter:

- Filter Name—Indicates the filter name.
- Device ID—Indicates the device ID.
- LAG—Indicates the controller LAG status as true or false.
- Management IP—Indicates the management interface IP address of the controller.
- Management VlanId—Indicates the management VLAN Id of the controller.
- Management Netmask—Indicates the netmask mask of the management interface of the controller.
- Management Gateway—Indicates the netmask gateway of the management interface of the controller.
- AP Mgr IP—Indicates the IP address of the access point manager.
- AP Mgr Vlan Id—Indicates the VLAN identifier of the access point manager.
- AP Mgr Netmask—Indicates the netmask mask of the access point manager.
- AP Mgr Gateway—Indicates the gateway IP address of the access point manager.
- Status—Idle, Trap Received, Failed In Trap Processing, Failed In Applying Templates, Failed In Discovery Switch, Managed, Managed partially applied templates, or Unknown Error.
- Country—Indicates the country.
- Mobility Grp—Indicates the name of the mobility group.
- Mobility Grp Members—Indicates the members of the mobility group.
- Timestamp—Indicates the date and time of the information.

Listing All Auto Provisioning Filter(s) Device Information

To view details for all Auto Provisioning Filters, follow these steps:

Step 1 Choose **Configure > Controller Auto Provisioning**.

Step 2 From the Select a command drop-down list, choose **List All Filter(s) Device Info**.

Step 3 Click **Go**.

The following information is provided for the selected filter:

- Filter Name—Indicates the filter name.
- Device ID—Indicates the device ID.
- LAG—Indicates the controller LAG status as true or false.
- Management IP—Indicates the management interface IP address of the controller.
- Management VlanId—Indicates the management Vlan Id of the controller.
- Management Netmask—Indicates the netmask mask of the management interface of the controller.
- Management Gateway—Indicates the netmask gateway of the management interface of the controller.
- AP Mgr IP—Indicates the IP address of the access point manager.
- AP Mgr Vlan Id—Indicates the Vlan identifier of the access point manager.
- AP Mgr Netmask—Indicates the netmask mask of the access point manager.
- AP Mgr Gateway—Indicates the gateway IP address of the access point manager.
- Status—Idle, Trap Received, Failed In Trap Processing, Failed In Applying Templates, Failed In Discovery Switch, Managed, Managed partially applied templates, or Unknown Error.
- Country—Indicates the country.
- Mobility Grp—Indicates the name of the mobility group.
- Mobility Grp Members—Indicates the members of the mobility group.
- Timestamp—Indicates the date and time of the information.

Exporting Auto Provisioning Filter(s)

To export an Auto Provisioning Filter, follow these steps:

Step 1 Choose **Configure > Controller Auto Provisioning**.

Step 2 Select the check box of the filter(s) you want to export.

Step 3 From the Select a command drop-down list, choose **Export Filter(s) Config (CSV)**.

Step 4 Click **Go**.

Step 5 In the File Download dialog box that appears, click **Save** to save the file to a location on the computer.

Exporting All Auto Provisioning Filter(s)

To export all Auto Provisioning Filters, follow these steps:

Step 1 Choose **Configure > Controller Auto Provisioning**.

Step 2 From the Select a command drop-down list, choose **Export All Filter(s) Config (CSV)**.

Step 3 Click **Go**.

Step 4 In the File Download dialog box that appears, click **Save** to save the file to a location on the computer.

Auto Provisioning Primary Search Key Settings

The Primary Search Key Setting enables you to set the matching criteria search order.

To indicate the Search Key Order, follow these steps:

Step 1 Choose **Configure > Controller Auto Provisioning**.

Step 2 From the left sidebar menu, choose **Setting**.

Step 3 Click to highlight the applicable search key.

Step 4 Use the **Move Up** or **Move Down** buttons to move the search key to a higher or lower priority.

Step 5 Click **Save** to confirm or **Cancel** to cancel the changes.

Configuring wIPS Profiles

The NCS provides several pre-defined profiles from which to choose. These profiles (based on customer types, building types, industry types, and so on) allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. You can use a profile 'as is' or customize it to better meet your needs.

Tip To learn more about Cisco Adaptive wIPS features and functionality, go to Cisco.com to watch a multimedia presentation. Here you find learning modules for a variety of the NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

Pre-defined profiles include the following:

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

The wIPS Profiles page provides access to the wIPS profile list and the SSID group list. To access the wIPS Profile page, choose **Configure > wIPS Profiles**.

The current wIPS profile list and the SSID group list can be accessed from the left sidebar menu.

The wIPS Profiles page defaults to the Profile List. The SSID Group List page is accessible from the left sidebar menu.

Note Adaptive wIPS does not support the NCS partitioning feature.

Profile List

The wIPS Profiles > Profile List page allows you to view, edit, apply, or delete current wIPS profiles and to add new profiles.

Tip To learn more about Cisco Adaptive wIPS features and functionality, go to Cisco.com to watch a multimedia presentation. Here you also find learning modules for a variety of the NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

To access the wIPS profile list for the NCS, choose **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List. If the Profile List is not currently displayed, choose **Profile List** from the wIPS Profiles left sidebar menu.

The Profile List provides the following information for each profile:

- Profile Name—Indicates the user-defined name for the current profile. Click the profile name to view or edit profile details.

Note When you hover your mouse cursor over the profile name, the Profile ID and version appear.

- MSE(s) Applied To—Indicates the number of mobility services engines (MSEs) to which this profile is applied. Click the MSE number to view profile assignment details.
- Controller(s) Applied To—Indicates the number of controllers to which this profile is applied. Click the controller number to view profile assignment details.

This section contains the following topics:

- Adding a Profile, page 8-238
- Deleting a Profile, page 8-241
- Applying a Current Profile, page 8-242

The profile editor allows you to create new or modify current profiles. See the "Profile Editor" section on page 8-239 for more information.

Adding a Profile

A new wIPS profile can be created using the default or a pre-configured profile.

Tip To learn more about Cisco Adaptive wIPS features and functionality, go to Cisco.com to watch a multimedia presentation. Here you also find learning modules for a variety of the NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

To add a wIPS profile, follow these steps:

Step 1 Select **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List.

Step 2 From the Select a command drop-down list, choose **Add Profile**.

Step 3 Click **Go**.

Step 4 Type a profile name in the Profile Name text box of the Profile Parameters page.

Step 5 Select the applicable pre-defined profile, or choose **Default** from the drop-down list. Pre-defined profiles include the following:

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

Step 6 Select one of the following:

- Save—Saves the profiles to the NCS database with no changes and no mobility services engine or controller assignments. The profile appears in the profile list.
- Save and Edit—Saves the profile and allows you to edit the profile.
- Cancel—Closes the Profile Parameters page without creating a profile.

Profile Editor

Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html
Here you also find learning modules for a variety of the NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

The profile editor allows you to configure profile details including the following:

- SSID groups—Add, edit, or delete SSID groups.
- Policy inclusion—Determine which policies are included in the profile.
- Policy level settings—Configure settings for each policy such as threshold, severity, notification type, and ACL/SSID groups.

- MSE/controller applications—Select the mobility services engine(s) or controller(s) to which you want to apply the profile.

To configure profile details, follow these steps:

Step 1 Access the profile editor. This can be done in two ways:

- When creating a new profile, click **Save and Edit** in the Profile Parameters page.
- Click the profile name from the Profile List page.

Step 2 From the SSID Groups page, you can edit and delete current groups or add a new group. For more information on adding, editing, or deleting SSID groups, see the "Configure > wIPS > SSID Group List" section on page 8-242 for more information.

Step 3 When SSID groups have been added or edited as needed, select one of the following:

- Save—Saves the changes made to the SSID groups.
- Cancel—Returns to the profile list with no changes made.
- Next—Proceeds to the Profile Configuration page.

Step 4 From the Profile Configuration page, you can determine which policies are included in the current profile. The check boxes in the policy tree (located in the left Select Policy pane) indicate which policies are enabled or disabled in the current profile. You can enable or disable an entire branch or an individual policy as needed by selecting the check box for the applicable branch or policy.

Note By default, all policies are selected.

Note For detailed information regarding each of the wIPS policies, see the "wIPS Policy Alarm Encyclopedia" section on page 17-1.

Step 5 In the Profile Configuration page, click an individual policy to display the policy description and to view or modify current policy rule settings.

The following options are available for each policy:

- Add—Click **Add** to access the Policy Rule Configuration page to create a new rule for this policy.
- Edit—Select the check box of the applicable rule, and click **Edit** to access the Policy Rule Configuration page to edit the settings for this rule.
- Delete—Select the check box of the rule you want to delete, and click **Delete**. Click **OK** to confirm the deletion.

  Note There must be at least one policy rule in place. You cannot delete a policy rule if it is the only one in the list.

- Move Up—Select the check box of the rule you want to move up in the list. Click **Move Up**.
- Move Down—Select the check box of the rule you want to move down in the list. Click **Move Down**.

The following settings can be configured at the policy level:

- Threshold (not applicable to all policies)—Indicates the threshold or upper limit associated with the selected policy. When the threshold is reached for a policy, an alarm is triggered.

Note Because every policy must contain at least one threshold, default thresholds are defined for each based on standard wireless network issues.

Note Threshold options vary based on the selected policy.

Note Alarms from Cisco Adaptive wIPS DoS and security penetration attacks are classified as security alarms. A summary of these attacks is located in the Security Summary page. Choose **Monitor > Security** to access this page. The wIPS attacks are located in the Threats and Attacks section.

- Severity—Indicates the level of severity of the selected policy. Parameters include critical, major, info, and warning. The value of this field might vary depending on the wireless network.
- Notification—Indicates the type of notification associated with the threshold.
- ACL/SSID Group—Indicates the ACL or SSID Group(s) to which this threshold is be applied.

Note Only selected groups trigger the policy.

Step 6 When the profile configuration is complete, select one of the following:

- Save—Saves the changes made to the current profile.
- Cancel—Returns to the profile list with no changes made.
- Back—Returns to the SSID Groups page.
- Next—Proceeds to the MSE/Controller(s) page.

Step 7 In the Apply Profile page, select the check box(es) of the mobility services engine and controller(s) to which you want to apply the current profile.

Step 8 When the applicable mobility services engine(s) and controller(s) are selected, choose one of the following:

- Apply—Applies the current profile to the selected mobility services engine/controller(s).
- Cancel—Returns to the profile list with no changes made.

Note A created profile can also be applied directly from the profile list. From the Profile List page, select the check box of the profile you want to apply and click **Apply Profile** from the Select a command drop-down list. Click **Go** to access the Apply Profile page.

Deleting a Profile

To delete a wIPS profile, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List.

Step 2 Select the check box of the wIPS profile(s) you want to delete.

Step 3 From the Select a command drop-down list, choose **Delete Profile**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Note If the profile is already applied to a controller, it cannot be deleted.

Applying a Current Profile

Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html
Here you also find learning modules for a variety of the NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

To apply a wIPS profile, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List.

Step 2 Select the check box of the wIPS profile(s) you want to apply.

Step 3 From the Select a command drop-down list, choose **Apply Profile**.

Step 4 Click **Go**.

Step 5 Select the mobility services engine(s) and controller(s) to which the profile is applied.

Note If the new assignment is different than the current assignment, you are prompted to save the profile with a different name

Step 6 When the applicable mobility services engine(s) and controller(s) are selected, choose one of the following:

- Apply—Applies the current profile to the selected mobility services engine/controller(s).
- Cancel—Returns to the profile list with no changes made.

Configure > wIPS > SSID Group List

The SSID (Service Set IDentifier) is a token or key which identifies an 802.11 (Wi-Fi) network. You must know the SSID to join an 802.11 network. SSIDs can be associated with a wIPS profile as a group using the SSID group list feature.

An SSID group can be added to a profile by importing it from the Global SSID Group List page (Configure > wIPS Profiles > SSID Group List) or by adding one directly from the SSID Groups page.

This section contains the following topics:

Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html
Here you also find learning modules for a variety of the NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

Global SSID Group List

The SSID Group List page allows you to add or configure global SSID groups that you might later import into an applicable wIPS profile.

Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html
Here you also find learning modules for a variety of the NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

To access the SSID Group List page, choose **Configure > wIPS Profiles**. From the left sidebar menu, choose **SSID Group List**. The SSID Group List page display current SSID groups and their associated SSIDs.

This section contains the following topics:

Adding a Group

To add an SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **SSID Group List**.

Step 3 From the Select a command drop-down list, choose **Add Group**.

Step 4 Click **Go**.

Step 5 In the SSID configuration page, type an SSID group name in the available text box.

Step 6 Enter the SSIDs in the SSID List text box. Separate multiple SSIDs with a space.

Step 7 When finished, select one of the following:

- Save—Saves the SSID group and adds it to the SSID Group List.
- Cancel—Closes the SSID configuration page without saving the new SSID group.

Note To import the SSID groups to a profile, choose **Configure > wIPS Profile**. Click the profile name for the applicable profile to open the SSID Groups page. From the Select a command drop-down list, choose **Add Groups from Global List**. Select the check box(es) for the SSID group(s) you want to import and click **Save**.

Editing a Group

To edit a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **SSID Group List**.

Step 3 Select the check box of the SSID group that you want to edit.

Step 4 From the Select a command drop-down list, choose **Edit Group**.

Step 5 Click **Go**.

Step 6 In the SSID configuration page, make the necessary changes to the SSID group name or the SSID list.

Step 7 When finished, select one of the following:

- Save—Saves the current changes and closes the SSID configuration page.
- Cancel—Closes the SSID configuration page without saving the changes.

Deleting a Group

To delete a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **SSID Group List**.

Step 3 Select the check box of the SSID group(s) that you want to delete.

Step 4 From the Select a command drop-down list, choose **Delete Group**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion.

SSID Groups

The SSID Groups page is the first page displayed when you access the profile editor. This page displays SSID groups that are included for the current wIPS profile.

From this page, you can add, import, edit, or delete an SSID group for the current profile.

Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html
Here you also find learning modules for a variety of the NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

This section contains the following topics:

Adding a Group

To add an SSID Group to the current wIPS profile, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **Profile List**.

Step 3 Click the profile name of the applicable wIPS profile.

Step 4 From the Select a command drop-down list, choose **Add Group**.

Step 5 Click **Go**.

Step 6 In the SSID configuration page, type an SSID group name in the available text box.

Step 7 Enter the SSIDs in the SSID List text box. Separate multiple SSIDs with a comma.

Step 8 When finished, select one of the following:

- Save—Saves the SSID group and adds it to the SSID Group List.
- Cancel—Closes the SSID configuration page without saving the new SSID group.

Adding Groups from Your Global List

SSID groups can also be added by importing them from your Global SSID Groups list. See the "Global SSID Group List" section on page 8-243 for more information on creating a global SSID groups list.

To import SSID groups into a profile, follow these steps:

Step 1 Select **Configure > wIPS Profile**.

Step 2 Click the profile name for the applicable profile to open the SSID Groups page.

Step 3 From the Select a command drop-down list, choose **Add Groups from Global List**.

Step 4 Select the check box(es) for the SSID group(s) you want to import.

Step 5 Click **Save**.

Editing a Group

To edit a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **Profile List**.

Step 3 Click the profile name of the applicable wIPS profile.

Step 4 Select the check box of the SSID group that you want to edit.

Step 5 From the Select a command drop-down list, choose **Edit Group**.

Step 6 Click **Go**.

Step 7 In the SSID configuration page, make the necessary changes to the SSID group name or the SSID list.

Step 8 When finished, select one of the following:

- Save—Saves the current changes and closes the SSID configuration page.
- Cancel—Closes the SSID configuration page without saving the changes.

Deleting a Group

To delete a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **Profile List**.

Step 3 Click the profile name of the applicable wIPS profile.

Step 4 Select the check box of the SSID group that you want to delete.

Step 5 From the Select a command drop-down list, choose **Delete Group**.

Step 6 Click **Go**.

Step 7 Click **OK** to confirm the deletion.

Configuring ACS View Servers

To facilitate communication between the NCS and the ACS View Server and to access the ACS View Server tab, you must add a view server with credentials.

Note The NCS only supports ACS View Server 5.1 or later.

To configure the ACS View Server Credentials, follow these steps:

Step 1 Choose **Configure > ACS View Server**.

Step 2 Enter the port number of the ACS View Server you are adding. (Some ACS View Servers do not allow you to change the port on which HTTPS runs.)

Step 3 Enter the password that was established on the ACS View Server. Confirm the password.

Step 4 Specify the time in seconds after which the authentication request times out and a retransmission is attempted by the controller.

Step 5 Specify the number of retries to be attempted.

Step 6 Click **Submit**.

Configuring ACS View Server Credentials

To facilitate communication between the NCS and the ACS View Server and to access the ACS View Server tab, you must add a view server with credentials.

To configure the ACS View Server Credentials, follow these steps:

Note The NCS only supports ACS View Server 5.1 or later.

Step 1 Choose **Configure > ACS View Server**.

Step 2 Enter the port number of the ACS View Server you are adding. (Some ACS View Servers do not allow you to change the port on which HTTPS runs.)

Step 3 Enter the password that was established on the ACS View Server. Confirm the password.

Step 4 Specify the number of retries to be attempted.

Step 5 Click **Submit**.

Configuring TFTP or FTP Servers

Choose **Configure > TFTP/FTP Servers** to add or delete TFTP or FTP servers from the NCS.

Note The NCS uses an integral TFTP/FTP server. This means that third-party TFTP or FTP servers cannot run on the same workstation as the NCS, because the NCS and the third-party TFTP or FTP servers use the same communication port.

This section contains the following topics:

Adding a TFTP or FTP Server

To add a TFTP or FTP server, follow these steps:

Step 1 Choose **Configure > TFTP/FTP Servers**.

Step 2 From the Select a command drop-down list, choose **Add TFTP/FTP Server**.

Step 3 From the Server Type drop-down list, choose **TFTP**, **FTP**, or **Both**.

Step 4 Enter a TFTP/FTP server name. This is a user-defined name for the server.

Step 5 Enter the IP address of the TFTP/FTP server.

Step 6 Click **Save**.

Deleting TFTP or FTP Servers

To delete a TFTP or FTP server, select the check box for the applicable server, and choose **Delete TFTP/FTP Servers** from the Select a command drop-down list. Click **Go** and then click **OK** to confirm the deletion.

Interactive Graphs

This section contains the following topics:

Interactive Graphs Overview

Interactive graph features are based on Adobe Flex technology that uses flash to render the graphs on the browser and provide interactivity to the user.

Minimum Requirements include the following:

- Windows—Flash Player version 9.0.115.0.
- Linux—Flash Player version 9.0.115.0.

Note If you do not have a flash player or your version is not recent enough, an error page prompts you with this information. Click the **Get Latest Flash Player** link to access Adobe website. From this site, you can download the latest version of the flash player. You only need to download the flash player once. Remember to restart the browser following the download.

The NCS Interactive Graphs include line, area, pie, and stacked bar graphs.

Interactive Graph Features

Interactive graph features include the following:

- Two distinct types of graphs:
  - Time-based Graphs
  - Non-Time based

- Support for automatic refresh—The graphs refresh automatically within a predetermined interval of time.
- Two graph views:
  - Graph (Chart) view (default)
  - Table (Grid) view

Note Use the two toggle buttons located at the bottom left side of the graph page to switch between the two graph views. To view the button type, hover your mouse cursor over the applicable button for a tool tip identifying View in Chart or View in Grid. Click **View in Chart** to view the data in a graph. Click **View in Grid** to view the data in a table.

- Enlarged View—Click the button located at the bottom right side of the graph to enlarge the graph in a separate page. The Chart View and Grid View buttons are available in the new page to change the type of graph displayed.

Time-based Graphs

For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed. The time-frame options include the following:

- 6h—Denotes the last six hours of data from the current time. The data is gathered from the current database table.
- 1d—Denotes the last day (24 hours) of data from the current time. The data is gathered from the current database table.
- 1w—Denotes the last week (seven days) of data from the current time. The data is gathered from the hourly aggregated table.
- 2w—Denotes the last two weeks of data from the current time. The data is gathered from the hourly aggregated table.
- 4w—Denotes the last four weeks of data from the current time. The data is gathered from the hourly aggregated table.
- 3m—Denotes the last three months of data from the current time. The data is gathered from the daily aggregated table.
- 6m—Denotes the last six months of data from the current time. The data is gathered from the weekly aggregated table.
- 1y—Denotes the past year (12 months) of data from the current time. The data is gathered from the weekly aggregated table.
- Custom—User-selected time period. Both days and hours can be set for the start and end dates. The use of a current or hourly, daily, or weekly aggregated source for data depends upon the selected start date.

Note The data management settings for aggregated tables are located in the "Configuring Administrative Settings" section on page 15-51 on the Administration menu. The default settings have a value of 31 days for Daily Aggregated Data and ten weeks for Weekly Aggregated Data.

For more information on Interactive Graphs, see the "Interactive Graphs" section on page 8-248.

CHAPTER 9

Managing Clients

A client is a device that is connected to an access point or a switch. The NCS supports both wired and wireless clients. After you add controllers and switches to the NCS, the client discovery process starts. Wireless clients are discovered from managed controllers or autonomous access points. The wireless client count includes autonomous clients as well. Only in the case of switches, the NCS polls for clients immediately after the device is added. In the case of controllers, these are polled during regular client status poll. The NCS gets the client information from the switch and updates this information in the database. For wired clients, the client status polling to discover client associations occurs every two hours (by default). A complete polling happens twice every day to poll complete information of all wired clients connected to all switches.

The NCS uses background tasks to perform the data polling operations. There are three tasks associated with clients:

1. Autonomous AP Client Status
2. Lighweight Client Status
3. Wired Client Status

Note You can refresh the data collection tasks (such as polling interval) from the Administration > Background Tasks page. For details, see the "Performing Background Tasks" section on page 15-1.

Note The NCS enables you to track clients and be notified when these clients connect to the network. For details, see the "Tracking Clients" section on page 9-31.

Note For more information about enabling traps and syslogs on switches for wired client discovery, see the "Tracking Clients" section on page 9-31.

Not all users or devices are authenticated via 802.1x (for example, printers). In such a case, a network administrator can assign a username to a device. For details, see the "Configuring Unknown Devices" section on page 8-209.

If a client device is authenticated to the network through web auth, the NCS might not have username information for the client (applicable only for wired clients).

Client status (applicable only for wired clients) is noted as connected, disconnected, or unknown:

- Connected clients—Clients that are active and connected to a wired switch.

- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the SNMP connection to the wired switch is lost.

Note See the "Configuring Unknown Devices" section on page 8-209 for more information about tracking clients.

The NCS supports both identity and non-identity wired clients. The support for wired clients is based on the identity service. The identity service provides secure network access to users and devices and it also enables the network administrators to provision services and resources to the users based on their job functions.

This chapter contains the following sections:

Client Dashlets on the General Dashboard

Note The dashlets that you see on the dashboard are presented in the form of interactive graphs. See the "Interactive Graphs" section on page 8-248 for more information.

When you log into the NCS, the General dashboard displays a few client-related dashlets.

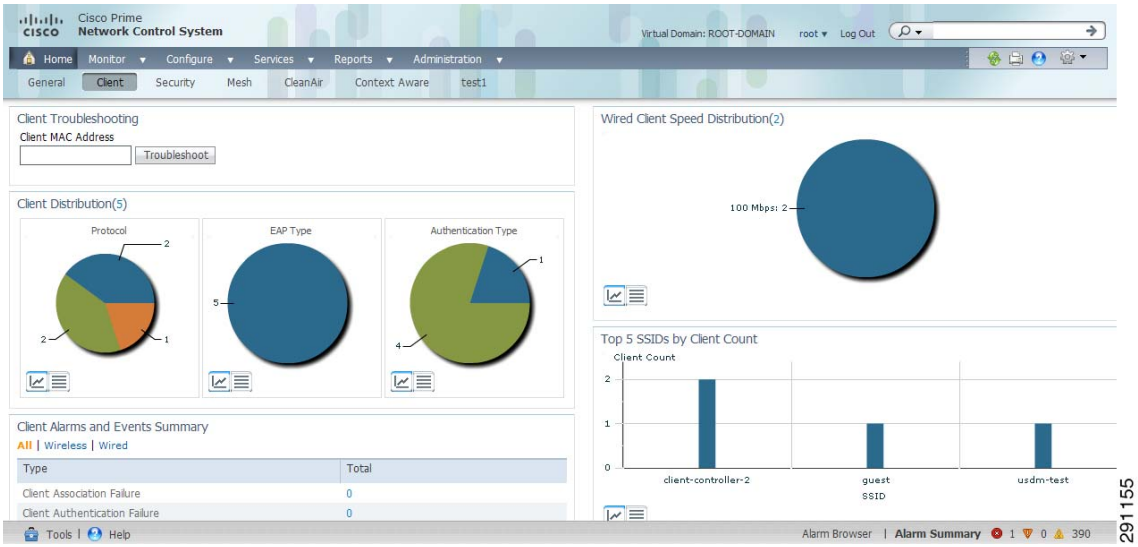
- Client Count By Association/Authentication—Displays the total number of clients by Association and authentication in the NCS over the selected period of time.
  - Associated client—All clients connected regardless of whether it is authenticated or not.
  - Authenticated client—All clients connected and passed authentication, authorization and other policies, and ready to use the network.
- Client Count By Wireless/Wired—Displays the total number of wired and wireless clients in the NCS over the selected period of time.

Client Dashboard

Note The dashlets that you see on the dashboard are presented in the form of interactive graphs. See the "Interactive Graphs" section on page 8-248 for more information.

The Client dashboard (see Figure 9-1) in the NCS home page displays the client-related dashlets. These dashlets enable you to monitor the clients on the network. The data for graphs is also polled/updated periodically and stored in the NCS database. On the other hand, most of the information in the Client Details page are polled directly from the controller/switch.

Figure 9-1 Client Dashboard



Click the **Edit Content** link to choose the dashlets you want to have appear on the Client dashboard. You can choose the dashlet from the Available dashlets list and then click to add it to the left or right column. For more information on using the Edit Content link, see the "Dashboards" section on page 2-13. For example, if you want to see the client count in both the General and Client dashboards, you can add the same dashlet to both.

To return to the original Client dashboard before customization, click **Edit Tabs**, and click **Reset to Factory Default**.

This section describes the Client dashboard dashlets and contains the following topics:

Client Troubleshooting Dashlet

To troubleshoot a client, enter a client MAC address, and then click **Troubleshoot** (see Figure 9-2). The properties information appears.

Figure 9-2 Client Troubleshooting

Note If the client is not currently associated, most of the information does not appear.

For details about client troubleshooting see the "Client Troubleshooting" section on page 9-22.

Client Distribution Dashlet

This dashlet (see Figure 9-3) shows how many clients are on your network presently. You can see how clients are distributed by protocol, EAP type, and authentication type.

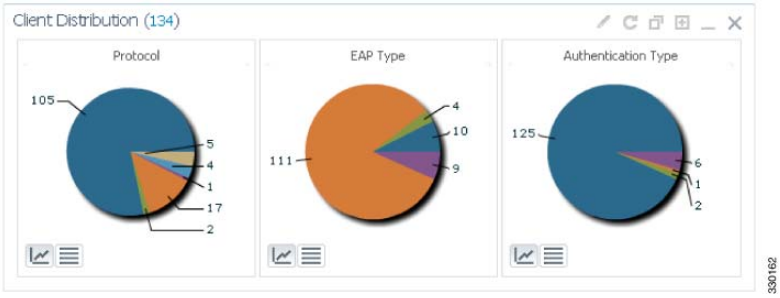
- Protocol
  - 802.11—wireless client protocol
  - 802.3—wired client protocol.

Note You can click a protocol to access the list of users belonging to that protocol. For example, if you click the 802.3 protocol, you can directly access the list of the wired clients and users in the Clients and Users page.

- EAP-Type—Represents Extensible Authentication Protocol (EAP) types such as EAP-FAST, PEAP, and so on
- Authentication Type—Represents types such as WPA (TKIP), WPA2 (AES), open, and so on

You can choose to display this information in table form or in a pie chart. The pie charts are clickable. If you hover your mouse cursor over a particular portion of the pie chart, a heading and percentage appears, and you can then click the pie chart piece to open a filtered list. When you click the number (next to the header 'Client Distribution') represented by Client Distribution, you get a list of clients represented by this number (the same page that you see when you choose Monitor > Clients and Users). You can filter the data that is displayed in client distribution by clicking the Dashlet Options icon and choosing either controller IP, SSID, or floor area.

Figure 9-3 Client Distribution

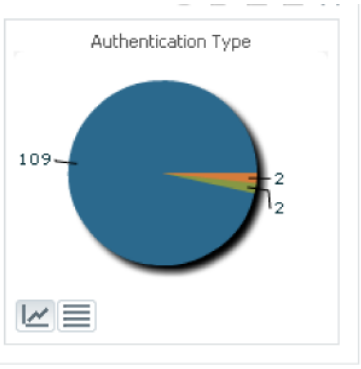


Note The *Edited* label next to the Client Distribution count indicates that the dashlet has been customized. If you reset to the default page, the *Edited* label is cleared.

Client Authentication Type Distribution

This Client Authentication Type graph shows the number of clients for each authentication type (see Figure 9-4). You can choose to display this information in table form or in a pie chart. When you click the number represented by Total Clients, you get a list of clients represented by this number (the same page that you see when you choose Monitor > Clients and Users). You can filter the data that is displayed in client authentication type distribution by clicking the Dashlet Options icon and choosing either controller IP, SSID, or floor area.

Figure 9-4 Client Authentication Type



Client Alarms and Events Summary Dashlet

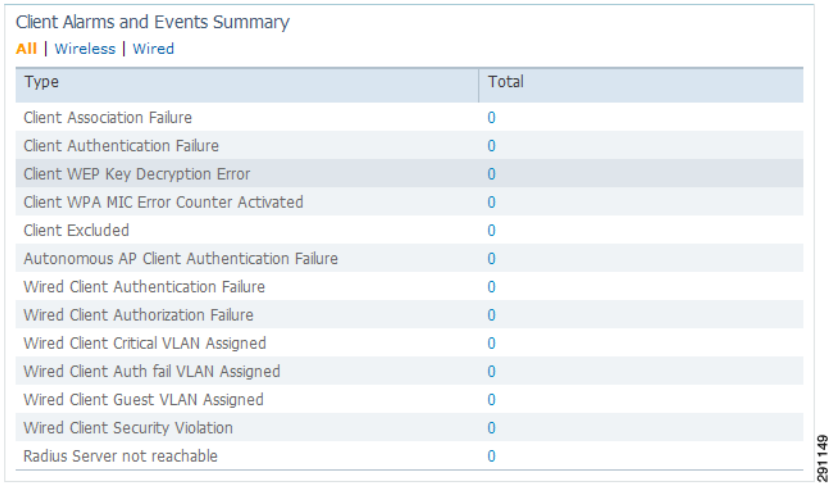
This dashlet (see Figure 9-5) shows the most recent client alarms of both wired and wireless clients.

- Client Association Failure
- Client Authentication Failure
- Client WEP Key Decryption Error
- Client WPA MIC Error Counter Activated
- Client Excluded
- Autonomous AP Client Authentication Failure
- Wired Client Authentication Failure
- Wired Client Authorization Failure
- Wired Client Critical VLAN Assigned
- Wired Client Auth fail VLAN Assigned
- Wired Client Guest VLAN Assigned
- Wired Client Security Violation

Note For more information about the alarms and events, see the "Alarm and Event Dictionary" section on page 13-1.

Click the number in the Total column to open the Events page (the same page that you see when you choose Monitor > Events).

Figure 9-5 Client Alarms and Events Summary

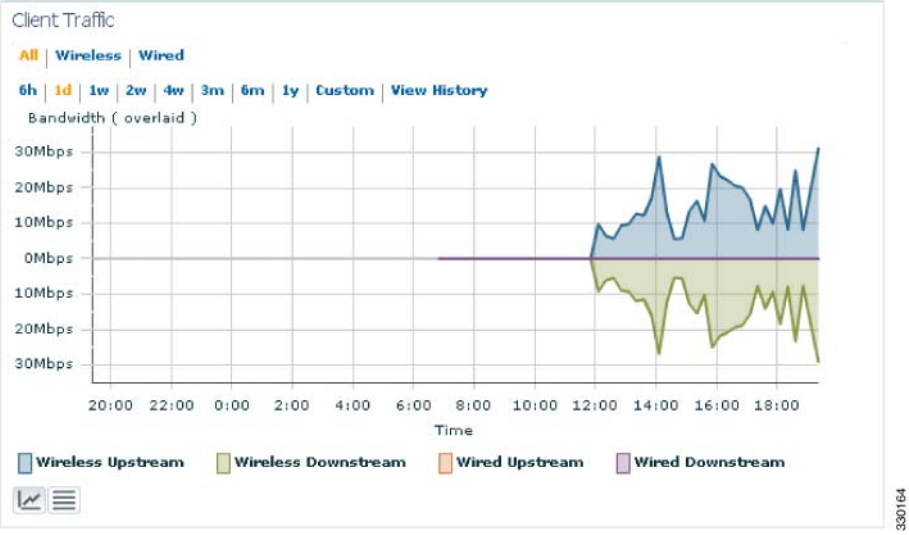


Client Traffic Dashlet

Controllers keep counters for the number of bytes transferred and received for each client. The NCS reads the number every 15 minutes and then calculates the difference, comparing the prior polling. This client traffic data is then aggregated every hour, every day, and every week (see Figure 9-6). It shows the average and maximum values in megabytes per second for both downstream and upstream traffic. You can display the information in table form or in an area chart. When generating the chart based on the floor, the NCS adds up all client traffic on this floor. You can filter the data that is displayed in client traffic by clicking the Dashlet Options icon and choosing either controller IP, SSID, or floor area.

For wireless clients, client traffic information comes from controller. For wired clients, the client traffic information comes form ISE, and therefore you need to enable accounting information and other necessary functions on switches.

Figure 9-6 Client Traffic



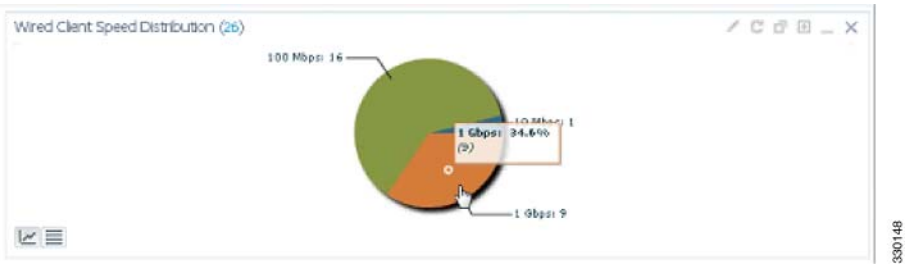
If you click **View History**, the Client Traffic Historical Charts dashlet appears for the various time frames. The Client Traffic Historical Charts dashlet shows the client traffic over the last 6 hours, last day, last week, last month, and last year. The blue line shows the authenticated client count and the orange line shows the associated client count. The upper right-hand corner shows when the chart was last updated.

Wired Client Speed Distribution Dashlet

This dashlet displays the wired client speeds and the client count for each speed. There are three different speeds on which clients run:

- 10 Mbps
- 100 Mbps
- 1 Gbps

Figure 9-7 Wired Client Speed Distribution

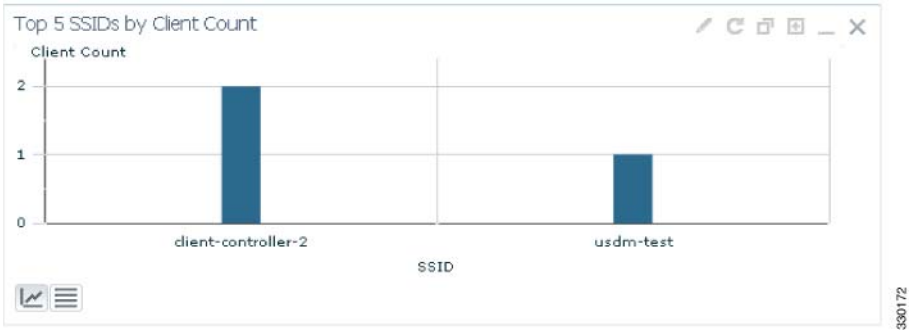


Note The ports are in the Auto Negotiate mode by default. For example, you get 100 Mbps speed for a client that runs in 100 Mbps speed.

Top 5 SSIDs by Client Count

This dashlet (see Figure 9-8) shows the count of currently associated and authenticated clients. You can choose to display the information in table form or in an area chart.

Figure 9-8 Top 5 SSIDs by Client Count

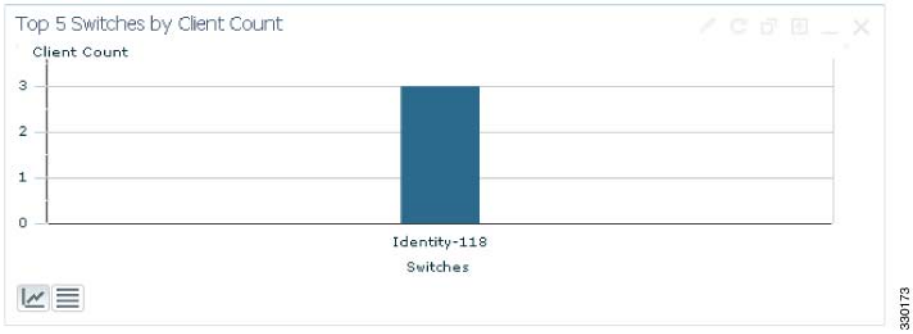


Note In the NCS 1.0, the WGB, Wired Guest, and OEAP 600 (Office Extended Access Point 600) are tracked as wireless clients.

Top 5 Switches by Switch Count

This dashlet (see Figure 9-9) displays the five switches that have the most clients as well as the number of clients associated to the switch.

Figure 9-9 Top 5 Switches by Switch Count Dashlet



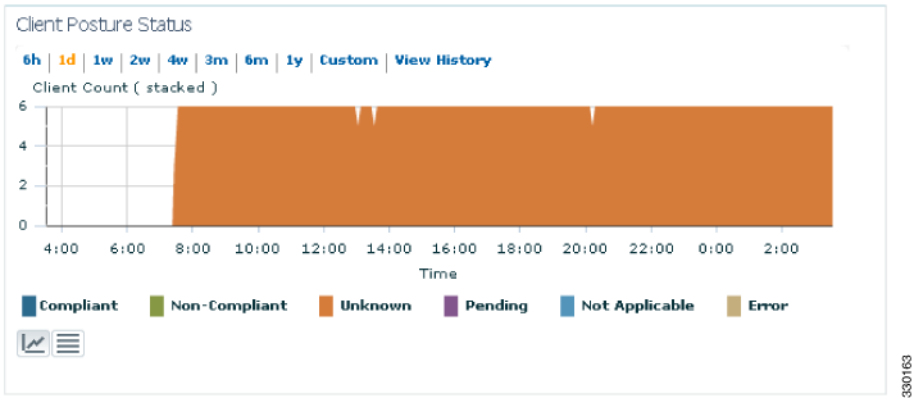
Client Posture Status Dashlet

The NCS collects the posture status information from the Identity Services Engine (ISE). You need to add an ISE for authorization and authentication purpose. For information about adding an ISE, see the "Adding an Identity Services Engine" section on page 11-103. After you enable necessary functions in ISE, the NCS shows the data in the Client Posture Status dashlet.

This dashlet (see Figure 9-10) displays the client posture status and the number of clients in each of the following status categories:

- Compliant
- Non-compliant
- Unknown
- Pending
- Not Applicable
- Error

Figure 9-10 Client Posture Status Dashlet



Monitoring Clients and Users

Using the Monitor Clients and Users feature, you can view all the clients in your network—both wired and wireless. In addition, you can view the client association history and statistical information. These tools are useful when users complain of network performance as they move throughout a building with their laptop computers. The information might help you assess what areas experience inconsistent coverage and which areas have the potential to drop coverage.

The Client Detail page shows the association history graph to represent the time-based data. The information helps you identify, diagnose, and resolve client issues.

Note Some of the features mentioned in this chapter are not applicable for wired clients (for example, disabling or removing).

Choose **Monitor > Clients and Users** to view both wired and wireless clients information. The Clients and Users page appears. In the Clients and Users page, you see the clients in tabular format with different tools available at the top of the table.

This section contains the following topics:

- Filtering Clients and Users, page 9-11
- Viewing Clients and Users, page 9-13
- Configuring the Search Results Display, page 9-33

Filtering Clients and Users

In the Clients and Users list page, all associated clients are displayed by default. There are 17 preset filters that allow you to view a subset of clients (see Table 9-1).

Note The WGB, Wired Guest, and OEAP 600 (Office Extended Access Point 600) are tracked as wireless clients.

Table 9-1 lists the preset filters that are available in the Clients and Users page. Choose the filter you want to show from the Show drop-down list.

Table 9-1 Client List Filters

Filter	Results
All	All clients including inactive clients.
2.4 GHz Clients	All clients using 2.4 GHz radio band.
5 GHz Clients	All clients using 5.0 GHz radio band.
All Lightweight Clients	All clients connected to lightweight APs.
All Autonomous Clients	All clients connected to autonomous APs.
All Wired Clients	All clients directly connected to a switch managed by the NCS.
Associated Clients	All clients connected to the network regardless of whether they are authenticated or not.
Clients detected by MSE	All clients detected by MSE including wired and wireless clients.
Clients detected in last 24 hours	All clients detected in the last 24 hours.
Clients Known by ISE	Shows all the clients that are authenticated by ISE.
Clients with Problems	Clients that are associated, but have not yet completed policy.
Excluded Clients	All lightweight wireless clients excluded by the controller.
FlexConnect Locally Authenticated	Clients connected to FlexConnect APs and authenticated locally.
New Clients detected in last 24 hours	New Clients detected in the last 24 hours.

Table 9-1 Client List Filters (continued)

Filter	Results
On Network Clients	Clients that have gone through authentication/authorization and are able to send and receive data. This means the clients that have completed all set policies and are on the network. The clients are not Identity clients and are always appear as 'On Network'.
WGB Clients	All WGB clients. **Note** If an access point is bridge capable, and the AP mode is set to Bridge, you can view clients identified as WGBs. WGB clients bridge wireless to wired. Any Cisco IOS access point can take on the role of a WGB, acting as a wireless client with a wired client connected to it. The information about this WGB is propagated to the controller and appears as a client in both the NCS and WLC.

In addition, you can use the filter icon ( ) to filter the records that match the filter rules. If you want to specify a filter rule, choose **All** from the Show drop-down list before you click .

Note When you select a preset filter and click the filter icon, the filter criteria is dimmed. You can only see the filter criteria but cannot change it. When the All option is selected to view all the entries, clicking the filter icon shows the quick filter options, where you can filter the data using the filterable fields. You can also enter text in the free form text box for table filtering.

Note When you perform advanced client filtering on IPv6 addresses, each octet that you specify must be a complete octet. If you specify a partial octet, the filtering might not show correct results. The following example shows how the advanced client filtering works on IPv6 addresses. This example assumes that you have the following IP addresses in the system:

```
10.10.40.1
10.10.40.2
10.10.40.3
10.10.240.1
Fec0::40:20
Fe80::240:20
```

If you search for all IP addresses containing 40, you get the following result:

```
10.10.40.1
```

```
10.10.40.2
10.10.40.3
Fec0::40:20
```

The IP addresses that contain 240 are not filtered because the filtering feature expects you to enter a complete octet.

Viewing Clients and Users

Note You can use the advanced search feature to narrow the client list based on specific categories and filters. See the "Using the Search Feature" section on page 2-33 section or the "Advanced Search" section on page 2-34 for more information.
You can also filter the current list using the Show drop-down list. See the " Filtering Clients and Users" section on page 9-11 for more information.

Note See the "Configuring the Search Results Display" section on page 9-33 for other available client parameters. See the " Filtering Clients and Users" section on page 9-11 for information on filtering this client list.

Note To view complete details in the Monitor > Client and Users page and to perform operations such as Radio Measurement, users in User Defined groups require permission before they access the Monitor Clients, View Alerts & Events, Configure Controllers, and Client Location pages.

To view clients and users, follow these steps:

Step 1 Choose **Monitor > Clients and Users** to view both wired and wireless clients information. The Clients and Users page appears.

The Clients and Users table displays a few columns by default. If you want display the additional columns that are available, click , and then click **Columns**. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.

The following columns are available in the Clients and Users table:

- MAC Address—Client MAC address.
- IP Address—Client IP address.

  The IP address that appears in the IP Address column is determined by a predefined priority order. The first IP address available in the following order appears in the IP address field:

  - IPv4 address.
  - IPv6 unique global address. If there are multiple addresses of this type, most recent IPv6 address the client received are shown, because a user can have two global IPv6 addresses but one might be from an older router advertisement that is being aged out.
  - IPv6 unique local address. If there are multiple IPv6 unique local addresses, the most recent one is used.

  - IPv6 link-local address. The IPv6 clients always have at least one link-local address.

  The following are the different IPv6 address types:

  - Link-local Unicast—The link-local addresses are designed to be used for addressing on a single link for purposes such as auto-address configuration, neighbor discovery, or when no routers are present.
  - Site-local Unicast—The site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix.
  - Global Unicast—The global unicast address uniquely identifies the client in the global network and is equivalent to a public IPv4 address. A client can have multiple global unicast addresses.

Note When there is more than one IP address of the same type, only the most recent IP address of that type appears, and the rest appear in the QuickView page when you hover your mouse cursor over the QuickView (+) icon.

- IP Address Type—The IP address type such as IPv4 and IPv6.
- Global Unique—The aggregate global unicast address of an IPv6 address. This field is populated only if a client is assigned a global unique IPv6 address.
- Unique Local—The local unicast address of an IPv6 address. This field is populated only if a client is assigned a local unique IPv6 address.
- Link Local—The link-local unicast address of an IPv6 address. This field is populated only if a client is assigned a link-local IPv6 address.
- User Name—Username based on 802.1x authentication or Web authentication. Unknown is displayed for a client connected without a username.
- Type—Indicates the client type.
  -  Indicates a lightweight client
  -  indicates a wired client
  -  Indicates an autonomous client
- Vendor—Device vendor derived from OUI.
- AP Name—Wireless only
- Device Name—Network authentication device name, for example, WLC, switch.
- Location—Map location of connected device.
- ISE—Yes/No. This column represents whether the client is authenticated using the ISE, which is added to the NCS.
- Endpoint Type—Endpoint type as reported by the ISE, available only when the ISE is added (for example, iPhone, iPad, Windows workstation).
- Posture—Latest client posture status
- SSID—Wireless only
- Profile Name—Wireless only
- VLAN——Indicates the access VLAN ID for this client.
- Status—Current client status
  - Idle—Normal operation; no rejections of client association requests.

  - Auth Pending—Completing a AAA transaction.
  - Authenticated—802.11 authentication complete.
  - Associated—802.11 association complete. This is also used by wired clients to represent that a client is currently connected to the network.
  - Power Save—Client is in power save mode.
  - Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.
  - To Be Deleted—The client that is deleted after disassociation.
  - Excluded—Automatically disabled by the system due to perceived security threat.
- Interface—Controller interface (wireless) or switch interface (wired) that the client is connected to.
- Protocol
  - 802.11—wireless
  - 802.3—wired
- Speed—Ethernet port speed (wired only). Displays “N/A” for wireless.
- Association Time—Last association start time (for wireless client). For a wired client, this is the time when the client is connected to a switch port. This column is blank for a client that is associated but has problems being on the network.
- Session Length—Session length.
- First Seen—Indicates the date and time when the client was first detected.
- Authentication Type—WPA, WPA2, 802.1x, MAC Auth Bypass, or Web Auth.
- Authorization Profile Names—Authorization profiles applied to this client by the ISE. This contains data only when the ISE is added and the client is authenticated by the ISE.
- Traffic (MB)—Traffic (transmitted/received) in this session in MB.
- Average Session Throughput (kbps)—Average session throughput in kbps.
- Automated Test Run—Indicates whether the client is in auto test mode. This is applicable for wireless clients only.
- AP MAC Address—Wireless only.
- AP IP Address—Wireless only.
- Anchor Controller—Lightweight wireless only.
- On Network—Shows Yes for the clients that are associated and have successfully finished authentication, if required.
- CCX—Lightweight wireless only.
- Client Host Name—Wired and wireless. Result of DNS reverse lookup.
- Device IP Address—IP address of the connected device (WLC, switch. or autonomous AP).
- Port—Switch port on WLC.
- E2E—Lightweight wireless only.
- Encryption Cipher—Wireless only.
- MSE—MSE server managing this client.
- RSSI—Wireless only.
- SNR—Wireless only.

- Router Advertisements Dropped—The router advertisements that are dropped for each client for a particular session.
- Session ID—Audit-session-ID used in the ISE and on the switch.
- FlexConnect Local Authentication—Indicates if the FlexConnect Local Authentication is enabled for this client.
- WGB Status—Indicates the status of the work group bridge mode.
- Mobility Status—Indicates the mobility status of the wireless client.
- SNMP NAC State—Indicates the state of the NAC appliance in out-of-band mode.

Step 2 Select a client or user. The following information appears:

- Client Attributes, page 9-16
- Client Statistics, page 9-17

Note Client Statistics shows statistical information after the client details are shown.

- Client Association History, page 9-18
- Client Event Information, page 9-19
- Client Location Information, page 9-19
- Wired Location History, page 9-19
- Client CCXv5 Information, page 9-20

The following attributes are populated only when the ISE is added to the NCS:

- ISE
- Endpoint Type
- Posture
- Authorization Profile Names

Note The NCS queries the ISE for client authentication records for the last 24 hours to populate this data. If the client is connected to the network 24 hours before it is discovered in the NCS, you might not see the ISE-related data in the table. You might see the data in client details page. To work around this, reconnect the client to the network. The ISE information is shown in the table after the next client background task run.

Client Attributes

When you select a client from the Clients and Users list, the client attributes appear in the Clients and Users list. Clients are identified using the MAC address.

Note The details that appear in the Client Attributes group box are from the device, whereas the details that appear in the Clients and Users list are from the database. Therefore, there can be some discrepancy between the details that appear in the Clients and Users list and the Client Attributes group box.

Note For wired clients, the information comes from the switch. Also, the data that appears in the details page is live data collected on demand from the controller/switch/ISE.

These details include the following client details:

- General—Lists the generation information such as User Name, MAC address, and so on.

  Note Click the ⊕ icon next to the username to access the correlated users of a user.

- Session—Lists the client session information.
- Security (wireless and Identity wired clients only)—Lists Security policy, authentication information, and EAP type.

  Note The identity clients are the clients whose authentication types are 802.1x, MAC Auth Bypass or Web Auth. For non-identity clients, the authentication type is N/A.

  Note The data that appears in the Client Attributes group box differs depending on the type of client: identity and non-identity clients. For identity clients, you can see the security information such as Authentication status, Audit Session ID, and so on.

- Statistics (wireless only)
- Traffic—Shows the client traffic information.

  Note For wireless clients, client traffic information comes from controller. For wired clients, the client traffic information comes form the ISE, therefore you must enable accounting information and other necessary functions on the switches.

Client IPv6 Addresses

When you select an IPv6 client from the Clients and Users list, the client IPv6 address details appear. These details come from the controller directly.

For the wired clients that have IPv6 addresses, the NCS discovers the client addresses from the IPv6 neighbors table on the switch.

These details include the following information:

- IP Address—Client IPv6 address.
- Scope
- Address Type
- Discovery Time

Client Statistics

The Client Statistics includes the following information for the selected client:

- Client AP Association History
- Client RSSI History (dBm)—History of RSSI (Received Signal Strength Indicator) as detected by the access point with which the client is associated.
- Client SNR History—History of SNR (signal-to-noise ratio of the client RF session) as detected by the access point with which the client is associated
- Bytes Sent and Received (Kbps)—Bytes sent and received with the associated access point.
- Packets Sent and Received (per second)—Packets sent and received with the associated access point.
- Data rate over time

Note Hover your mouse cursor over points on the graph for additional statistical information.

Note This information is presented in interactive graphs. See the "Interactive Graphs" section on page 8-248 for more information.

Client Association History

The Association History dashlet displays information regarding the last ten association times for the selected client. This information can help in troubleshooting the client.

- Client Association History (for wireless clients) includes the following information:
  - Date and time of association
  - Duration of association
  - Username
  - IP address
  - Access point name
  - Controller name
  - SSID
  - Protocol
  - Amount of traffic (MB)
  - Hostname
  - Roam reason (such as *No longer seen from controller* or *New association detected*)
- Client Association History (for wired clients) includes the following information:
  - Date and time of association
  - Duration of association
  - Username
  - IP address
  - Access point and controller name
  - Map location
  - SSID

- Protocol
- Amount of traffic (MB)
- Hostname
- Roam reason (such as *No longer seen from controller* or *New association detected*)

Note Click the **Edit View** link to add, remove or reorder columns in the Current Associated Clients table. See the "Configuring the List of Access Points Display" section on page 5-46 for adding new parameters than can be added through Edit View.

Client Event Information

The Client Event dashlet of the Client Details page displays all events for this client including the event type as well as the date and time of the event.

Click an event type to view its details. See the "Monitoring Failure Objects" section on page 5-152 for more information.

Client Location Information

The following location parameters appear (if available) for the selected client:

- Map Area—The map area in which the client was last located.
- ELIN—The Emergency Location Identification Number. This is applicable only to the wired clients that are located by MSE.
- Civic Address—The fields on the Civic Address tab are populated if a civic address is imported for a client. This is applicable only to the wired clients that are located by MSE.
- Advanced—Detailed information about the client. The fields on this tab are populated if a civic address is imported for a client.

For more information on importing Civic information for the client, see the "Configuring a Switch Location" section on page 8-206.

Wired Location History

You can view the Location History for wired clients.

Note The wired clients must be located by MSE and the history for wired clients must be enabled on the MSE.

The following Location History information is displayed for a client:

- Timestamp
- State
- Port Type
- Slot
- Module
- Port

- User Name
- IP Address
- Switch IP
- Server Name
- Map Location
- Civic Location

Wireless Location History

You can view the Location History for wireless clients.

Note The wireless clients must be located by MSE and the history for wired clients must be enabled on the MSE.

Client CCXv5 Information

CCXv5 clients are client devices that support Cisco Compatible Extensions Version 5 (CCXv5). Reports specific to CCXv5 clients provide client details that enhance client diagnostics and troubleshooting.

Note The CCXv5 manufacturing information is displayed for CCXv5 clients only.

To view specific client details, perform a client search using the applicable search parameters. For more information on performing a client search, see the "Client CCXv5 Information" section on page 9-20 or the "Advanced Search" section on page 2-34.

CCXv5 information is displayed in the Monitor Clients > Client Details page. CCXv5 information includes the following:

CCXv5 Manufacturing Information:

- Organizationally Unique Identifier—The IEEE assigned organizational unique identifier, for example, the first 3 bytes of the MAC address of the wireless network connected device.
- ID—The manufacturer identifier of the wireless network adapter.
- Model—Model of the wireless network adapter.
- Serial Number—Serial number of the wireless network adapter.
- Radio—Radio type of the client.
- MAC Address—MAC address assigned to the client.
- Antenna Type—Type of antenna connected to the wireless network adapter.
- Antenna Gain—The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.

Note Click **More** to view the following additional CCXv5 parameters.

Automated Troubleshooting Report—If the automated test runs, this report displays the location of automated troubleshooting log AUTO_TS_LOG<ClientMac>.txt. If no automated test runs, Not Exists appears.

- Click **Export** to save the .zip file. The file contains three logs: automated troubleshoot report, frame log, and watch list log.

Note The **Settings > Client** page allows you to enable automatic client troubleshooting on a diagnostic channel. This feature is only available for Cisco Compatible Extension clients version 5. See the "Processing Diagnostic Trap" section on page 15-56 for more information.

Radio Receiver Sensitivity—Displays receiver sensitivity of the wireless network adapter including the following:

- Radio
- Data Rate
- Minimum and Maximum RSSI

CCXV5 Capability Information—Displays the Capability Information parameters for CCXv5 clients only.

- Radio
- Client Status—Success or failure.
- Service Capability—Service capabilities such as voice, streaming (uni-directional) video, interactive (bi-directional) video.

Radio Channels—Identifies the channels for each applicable radio.

Transmit Data Rates—Identifies the transmission data rates (Mbps) for each radio.

Transmit Power Values—Identifies the transmission power values including:

- Power mode
- Radio
- Power (dBm)

Exporting Clients and Users

You can quickly export your clients and users list into a CSV file (spreadsheet format with comma-separated values).

Note The columns that are shown in the Clients and Users table are only exported to the CSV file.

To export the clients and users list, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Click the icon on the toolbar. A dialog box appears.

Step 3 In the File Download dialog box, click **Save**.

Client Troubleshooting

You can begin troubleshooting several ways: by entering a MAC address on the Client dashboard, by using the search function, or by selecting a row in the Monitor > Clients and Users page. Any of these methods provides all the information necessary to troubleshoot historical client issues. You can monitor the status of the connection, verify the current and past locations of a user, and troubleshoot client connectivity problems. You might want to use the client troubleshooting option if a user experiences repeated connectivity issues. The Client Details page shows SNR over time, RSSI over time, client reassociations, client reauthentications, and any RRM events. An administrator can correlate reassociations and reauthentications and determine if the problem was with the network or client.

Note You can troubleshoot current client issues only. You cannot troubleshoot the historic client issues. However, for location assisted clients, you can find the location history.

Note The client troubleshooting feature is available for identity wired clients only. This feature is not available for non-identity wired clients.

The NCS provides integrated management for wired and wireless devices or clients. You can monitor and troubleshoot both wired and wireless clients. SNMP is used to discover clients and collect client data. The ISE is polled periodically to collect client statistics and other attributes to populate related dashboard dashlets and reports. If the ISE is added to the systems and devices are authenticating to it, the Client Details page displays security information.

To launch the Client Troubleshooting tool, select a client, and then click the  icon indicated above the IP address that you want to troubleshoot. The Troubleshooting Client page appears.

The troubleshooting page displays the following states for wired clients:

- Link Connectivity
- 802.1X Authentication
- MAC Authentication
- Web Authentication
- IP Connectivity
- Authorization
- Successful Connection

Note The exact states displayed depend on the level of security used by the client.

The following are the security mechanisms used by clients:

- 802.1X
- MAC Authentication

- Web Authentication

Table 9-2 summarizes the validity of states against the security types. The states are arranged in the order the client goes through.

Table 9-2 Security Mechanisms

Security/Client State	Link Connectivity	802.1X Authentication	MAC Authentication	Web Authentication	IP Connectivity	Authorization
802.1X	X	X	–	–	X	X
MAC Authentication	X	–	X	–	X	X
Web Authentication	X	–	–	X	X	X

Table 9-3 provides the list of problems and suggested actions depending on the state in which a client failed:

Table 9-3 Client State, Problem, and Suggested Action

Client State	Problem	Suggested Action
Link Connectivity	Cannot find the client in network	• Check whether the client cable is plugged into the network • Check whether the client is using the proper cable to connect to the network • Make sure that the port to which client is connected is not disabled administratively. • Make sure that the port to which client is connected is not error disabled. • Check whether the speed and duplex are set to Auto on the port to which the client is connected.
	Authentication in progress	• If the client has been in this state for a long time, check the following: – Check whether the supplicant on the client is configured properly as required. – Modify the timers related to authentication method and try again. – If you are not sure which authentication method works with the client, use the fall back authentication feature. – Try disconnecting and reconnecting.

Table 9-3 Client State, Problem, and Suggested Action (continued)

Client State	Problem	Suggested Action
802.1X Authentication	802.1X Authentication Failure	• Check whether the RADIUS server(s) is reachable from the switch. • Check whether the client choice of EAP is supported by RADIUS server(s). • Check whether the username/password/certificate of the client is valid. • See whether the certificates used by RADIUS server are accepted by the client.
MAC Authentication	MAC Authentication Failure	• Check whether the RADIUS server(s) is reachable from the switch. • Check whether the MAC address of the client is in the list of known clients on the RADIUS server. • Check whether the MAC address of the client is not in the list of excluded clients.
Web Authentication	Client could not be authenticated through web/guest interface	• Check that the guest credentials are valid and not expired. • Check whether the client can be redirected to the login page. • Check whether the RADIUS server is reachable. • Confirm that pop-ups are not blocked. • Check that the DNS resolution on the client is working. • Check that the client is not using any proxy settings. • Check whether the client can access https://<virtual-ip>/login.html • Check whether the browser of the client accepts the self-signed certificate offered by the controller.

Table 9-3 Client State, Problem, and Suggested Action (continued)

Client State	Problem	Suggested Action
IP Connectivity	Client could not complete DHCP interaction	• Check whether the DHCP server is reachable. • Check whether the DHCP server is configured to serve the WLAN. • Check whether the DHCP scope is exhausted. • Check whether multiple DHCP servers are configured with overlapping scopes. • Check that the local DHCP server is present if DHCP bridging mode is enabled (move it to second) client is configured to get the address from the DHCP server. • Check if the client has static IP configured and ensure that the client generates IP traffic.
Authorization	Authorization Failure	• Check that the VLAN defined for authorization is available on the switch. • Check that the default port ACL is configured for ACL authorization.
Successful Connection	None	None.

Using the Search Feature to Troubleshoot Clients

Client search is the primary method used to locate clients. For a detailed description of the search feature, see to the "Using the Search Feature" section on page 2-33.

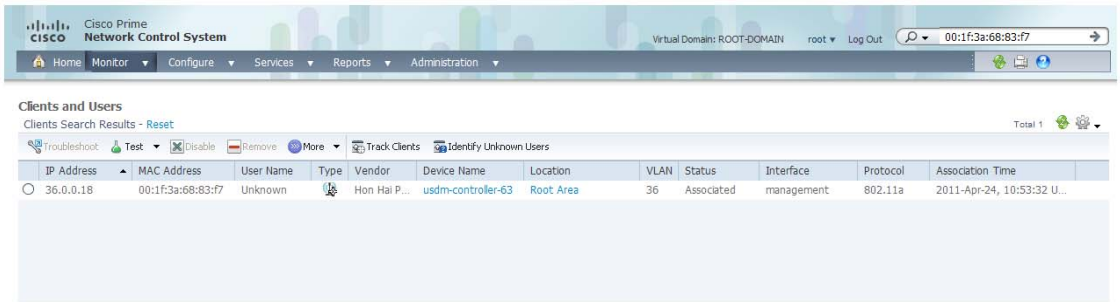
To troubleshoot a client using the Search feature, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Type the full or partial client MAC address in the Advanced Search text box, and click **Search**. The Search Results page appears.

Step 3 Click **View List** to see the clients that match the search criteria in the Clients page. The Monitor > Clients and Users page appears (see Figure 9-11).

Figure 9-11 Client and Users



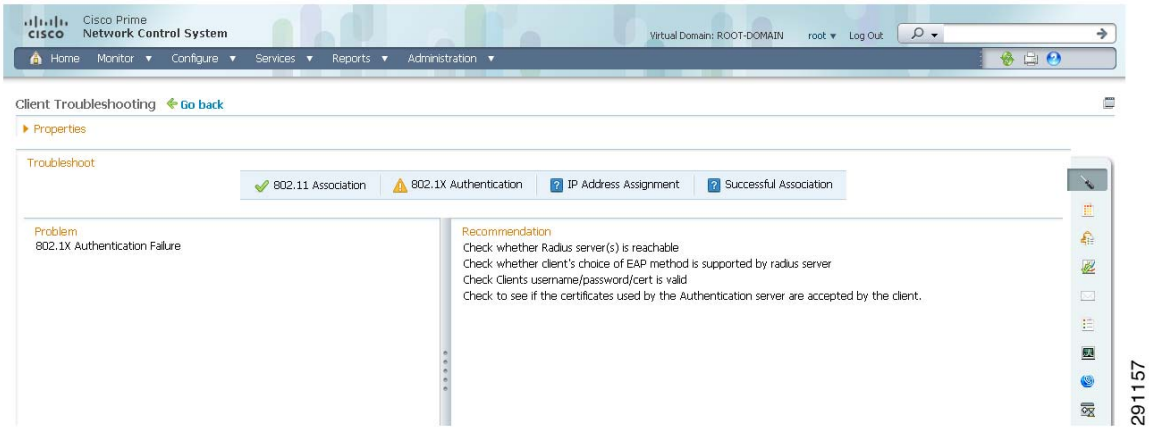
Note You can click the Reset link to set the table to the default display so that the search criteria is no longer applied.

Step 4 Select a client, and then click the icon indicated above the IP address that you want to troubleshoot. The Troubleshooting Client page appears (see Figure 9-12). If you are troubleshooting a Cisco Compatible Extension v5 client (wireless), your Troubleshooting Client page has additional tabs.

Note If you receive a message that the client does not seem to be connected to any access point, you must reconnect the client and click **Refresh**.

Note You can use the detach/clone icon located in the top right corner of the page to detach the current page into a new window/tab.

Figure 9-12 Troubleshooting Client Page



Note Click **Go back** to return to the page from where you launched client troubleshooting. For example, if you have launched client troubleshooting from the list page, you can return to the list page.

The summary page briefly describes the problem and recommends a course of action.

Note Some Cisco Compatible Extension features do not function properly when you use a web browser other than Mozilla Firefox 3.6 or later or Internet Explorer 7.0 or later on a Windows workstation.

Step 5 To view log messages logged against the client, click the **Log Analysis** tab (see Figure 9-13).

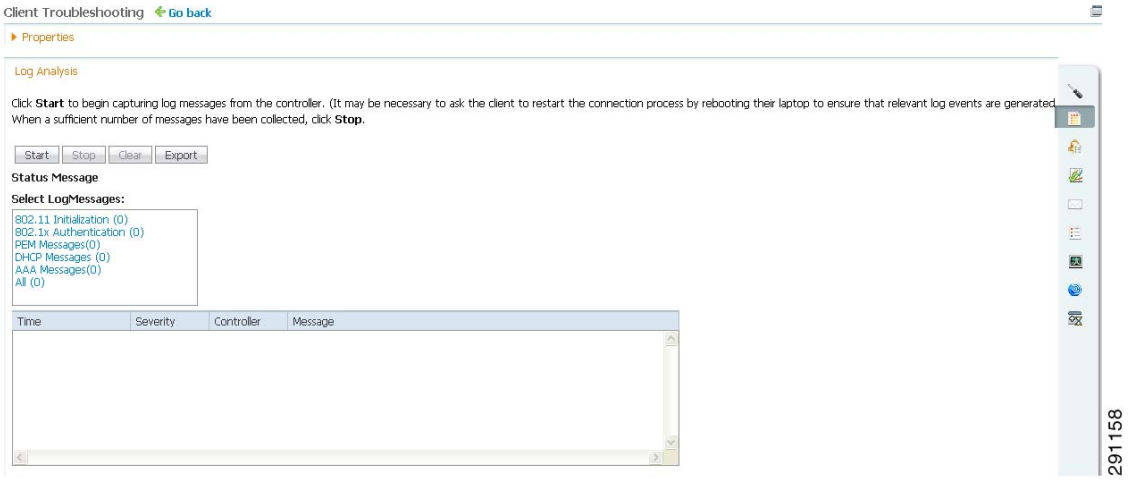
Step 6 To begin capturing log messages about the client from the controller, click **Start**. To stop log message capture, click **Stop**. To clear all log messages, click **Clear**.

Note Log messages are captured for ten minutes and then stopped automatically. You must click **Start** to continue.

Step 7 To select log messages to display, click one of the links under Select Log Messages (the number between parentheses indicates the number of messages). The messages appear in the group box. The message includes the following information:

- A status message
- The controller time
- A severity level of info or error (errors are displayed in red)
- The controller to which the client is connected

Figure 9-13 Log Analysis



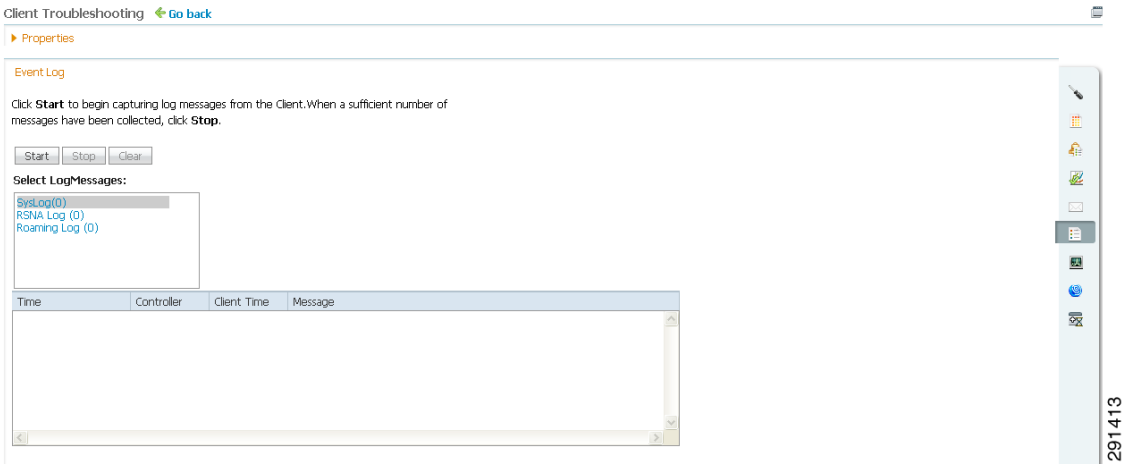
Step 8 To display the event history of a client, click the **Event History** tab (see Figure 9-14).

Event History provides messages related to connectivity events for this client. In this example (see Figure 9-14), the client failed to successfully authenticate. The date/time information is provided to assist the network administrator in troubleshooting this client.

Figure 9-14 Event History Tab

Step 9 To view the event log, click the **Event Log** tab (see Figure 9-15). Click **Start** to begin capturing log messages from the client. When a sufficient number of messages have been collected, click **Stop**.

Figure 9-15 Event Log



Note The Client Troubleshooting Event log and Messaging features are available to CCX Version 6 clients only if the Management Service version is 2 and later.

Step 10 If you click the ACS View Server tab, you can interact with the Cisco Access Control (ACS) System View Server. This tab displays the latest authentication records received either from an ACS View server or Identity Services Engine (ISE), whichever is configured in the NCS. You must have View Server credentials established before you can access this tab. (The tab shows the server list as empty if no view servers are configured.) See the "Configuring ACS View Server Credentials" section on page 8-247 for steps on establishing credentials.

If the ACS View Server is already configured, you can select a time range and click **Submit** to retrieve the authentication records from the ACS View Server. The NCS uses the ACS View NS API to retrieve the records.

Step 11 You can click the Identity Services Engine tab to view information about the ISE authentication. Enter the date and time ranges to retrieve the historical authentication and authorization information, and click **Submit**. The results of the query are displayed in the Authentication Records portion of the page.

Step 12 You can click the CleanAir tab to view information about the air quality parameters and the active interferers for the CleanAir enabled access point. This tab provides the following information about the air quality detected by the CleanAir-enabled access point.

- AP Name—Click to view the access point details. See the "Monitoring Access Points Details" section on page 5-57 for more information.
- AP MAC Address
- Radio
- CleanAir Capable—Indicates if the access point is CleanAir Capable.
- CleanAir Enabled—Indicates if CleanAir is enabled on this access point.
- Admin Status—Enabled or disabled.
- Operational Status—Displays the operational status of the Cisco Radio(s) (Up or Down).
- Channel—The channel upon which the Cisco Radio is broadcasting.
- Extension Channel—Indicates the secondary channel on which the Cisco Radio is broadcasting.

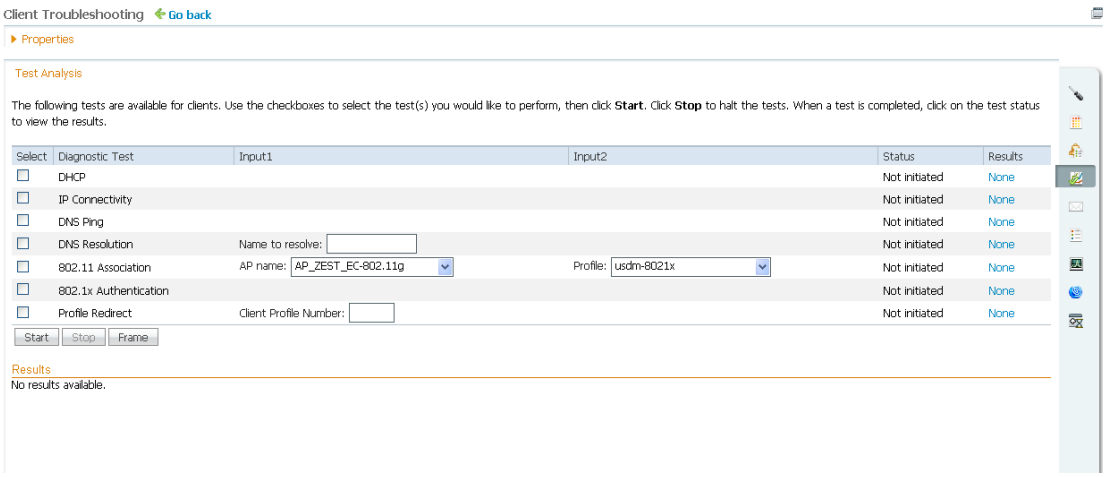
- Channel Width—Indicates the channel bandwidth for this radio interface. See the "Configuring 802.11a/n RRM Dynamic Channel Allocation" section on page 8-127 for more information on configuring channel bandwidth.
- Power Level—Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.
- The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.
- Average AQ Index—Average air quality index.
- Minimum AQ Index—Minimum air quality index.

The following information about the active interferers is displayed:

- Interferer Name—The name of the interfering device.
- Affected Channels—The channel the interfering device is affecting.
- Detected Time—The time at which the interference was detected.
- Severity—The severity index of the interfering device.
- Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.
- RSSI(dBm)—The Received Signal Strength Indicator of the interfering device.
- Click **CleanAir Details** to know more about the air quality index.

Step 13 (Optional) If Cisco Compatible Extension Version 5 or Version 6 clients are available, you can click the Test Analysis tab as shown in Figure 9-16.

Figure 9-16 Test Analysis Tab



Note The Client Troubleshooting Test Analysis feature is available to CCX Version 6 clients only if Management Service version is 2 and later.

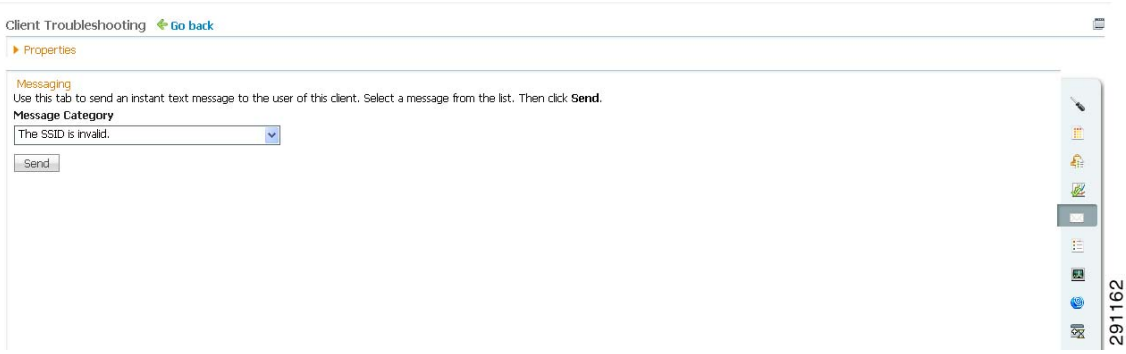
The Test Analysis tab allows you to run a variety of diagnostic tests on the client. Select the check box for the applicable diagnostic test, enter any appropriate input information, and click **Start**. The following diagnostic tests are available:

- DHCP—Executes a complete DHCP Discover/Offer/Request/ACK exchange to determine that the DHCP is operating properly between the controller and the client.
- IP Connectivity—Causes the client to execute a ping test of the default gateway obtained in the DHCP test to verify that IP connectivity exists on the local subnet.
- DNS Ping—Causes the client to execute a ping test of the DNS server obtained in the DHCP test to verify that IP connectivity exists to the DNS server.
- DNS Resolution—Causes the DNS client to attempt to resolve a network name known to be resolvable to verify that name resolution is functioning correctly.
- 802.11 Association—Directs an association to be completed with a specific access point to verify that the client is able to associate properly with a designated WLAN.
- 802.1X Authentication—Directs an association and 802.1X authentication to be completed with a specific access point to verify that the client is able to properly complete an 802.1x authentication.
- Profile Redirect—At any time, the diagnostic system might direct the client to activate one of the configured WLAN profiles and to continue operation under that profile.

Note To run the profile diagnostic test, the client must be on the diagnostic channel. This test uses the profile number as an input. To indicate a wildcard redirect, enter 0. With this redirect, the client is asked to disassociate from the diagnostic channel and to associate with any profile. You can also enter a valid profile ID. Because the client is on the diagnostic channel when the test is run, only one profile is returned in the profile list. You should use this profile ID in the profile redirect test (when wildcard redirecting is not desired).

Step 14 (Optional) If Cisco Compatible Extension Version 5 or Version 6 clients are available, a Messaging tab appears (see Figure 9-17). Use this tab to send an instant text message to the user of this client. From the Message Category drop-down list, choose a message, and click **Send**.

Figure 9-17 Messaging Tab



Note The Client Troubleshooting Event log and Messaging features are available to CCX Version 6 clients only if the Management Service version is 2 and later.

Step 15 You can click the **Identity Services Engine** tab to view information about the identity services parameters. You must have an Identity Services Engine (ISE) configured before you can access this tab. (The tab shows the server list as empty if no ISEs are configured.)

Note If the ISE is not configured it provides a link to add an ISE to the NCS.

The ISE provides authentication records to the NCS via REST API. The network administrator can choose a time period for retrieving authentication records from the ISE (see Figure 9-18).

Figure 9-18 Identity Services Engine Tab

Step 16 To view the client location history, click the **Context Aware History** tab (see Figure 9-19).

Figure 9-19 Identity Services Engine Tab

Step 17 Close the Troubleshooting Client page.

Tracking Clients

This feature enables you to track clients and be notified when these clients connect to the network.

To track clients, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Click **Track Clients**. The Track Clients dialog box appears listing the currently tracked clients.

Tip This table supports a maximum of 2000 rows. To add or import new rows, you must first remove some older entries.

Step 3 To track a single client, click **Add**, and then enter the following parameters:

- Client MAC address
- Expiration—Choose **Never** or enter a date.

Step 4 To track multiple clients, click **Import**. This allows you to import a client list from a CSV file. Enter MAC Address and username.

A sample CSV file can be downloaded that provides data format:

```
# MACAddress, Expiration: Never/Date in MM/DD/YYYY format
00:40:96:b6:02:cc,10/07/2010
00:02:8a:a2:2e:60,Never
```

Notification Settings

To specify notification settings for the tracked clients, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Click **Track Clients**. The Track Clients dialog box appears listing the currently tracked clients.

Step 3 Select the tracked client(s) for which you want to specify notification settings.

Step 4 Specify the notification settings. There are three options for notifications:

a. Purged Expired Entries—You can set the duration to keep tracked clients in the NCS database. Clients can be purged as follows:

- after 1 week
- after 2 weeks
- after 1 month
- after 2 months
- after 6 months
- kept indefinitely

b. Notification Frequency—You can specify when the NCS sends a notification of a tracked client:

- on first detection
- on every detection

c. Notification Method—You can specify that the tracked client event generates an alarm or sends an e-mail.

Step 5 Click **Save**.

Identifying Unknown Users

Not all users or devices are authenticated via 802.1x (for example, printers). In such a case, a network administer can assign a username to a device.

If a client device is authenticated to the network through web auth, the NCS might not have username information for the client (applicable only for wired clients).

Clients are marked as unknown when the NMSP connection to the wired switch is lost. A client status (applicable only for wired client) is noted as connected, disconnected, or unknown:

- Connected clients—Clients that are active and connected to a wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the NMSP connection to the wired switch is lost.

To view the unknown devices, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Click **Identify Unknown Users**.

Step 3 Click **Add** to assign client MAC addresses to username.

Step 4 Enter the MAC address and username.

Note Once a client and MAC address have been added, the NCS uses this data for client lookup based on the matching MAC address.

Step 5 Click **Add**.

Step 6 Repeat Step 3 to Step 5 to enter a MAC Address and its corresponding username for each client.

Step 7 Click **Save**.

Note This table supports a maximum of 10,000 rows. To add or import new rows, you must first remove some older entries.

Configuring the Search Results Display

The **Edit View** page allows you to add, remove, or reorder columns in the Clients table.

To edit the available columns in the Clients table, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Click the **Edit View** link.

Step 3 To add an additional column to the Clients table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the Clients table.

Step 4 To remove a column from the Clients table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. All items in the left column are not displayed in the Clients table.

Step 5 Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.

Step 6 Click **Reset** to restore the default view.

Step 7 Click **Submit** to confirm the changes.

Note Additional client parameters include: AP MAC Address, Anchor Controller, Authenticated, CCX, Client Host Name, Controller IP Address, Controller Port, E2E, Encryption Cipher, MSE, RSSI, SNR, and FlexConnect Local Authentication.

Enabling Automatic Client Troubleshooting

In the Settings > Client page, you can enable automatic client troubleshooting on a diagnostic channel. This feature is available only for Cisco Compatible Extension clients Version 5.

To enable automatic client troubleshooting, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Client**.

Step 3 Select the **Automatically troubleshoot client on diagnostic channel** check box.

Note When the check box is selected, the NCS processes the diagnostic association trap. When it is not selected, the NCS raises the trap, but automated troubleshooting is not initiated.

Step 4 Click **Save**.

Viewing Client Details in the Access Point Page

You can also view the client information from the access point page. Choose **Monitor > Access Points**. Click an access point URL from the column to see details about that access point. Click the **Current Associated Clients** tab.

Viewing Currently Associated Clients

You can also view the currently associated clients (wired) from the switch details page. Choose **Monitor > Controllers**, select an IP address, and choose **Clients > Current Associated Clients** from the left sidebar menu.

Running Client Reports

You can run client reports such as busiest clients, client count, client sessions, client summary, throughput, unique clients and v5 clients statistics from the Report Launch pad. See the "Creating and Running a New Report" section on page 14-6.

Running ISE Reports

You can also launch ISE reports from the Report Launch pad. See the "Creating and Running a New Report" section on page 14-6. For more information about running the ISE reports, see the ISE online help.

Specifying Client Settings

The Administration > Settings > Client page allows you to specify various client settings. For details, see "Configuring Clients" section on page 15-55.

Receiving Radio Measurements for a Client

In the client page, you can receive radio measurements only if the client is Cisco Compatible Extensions v2 (or higher) and is in the associated state (with a valid IP address). If the client is busy when asked to do the measurement, it determines whether to honor the measurement or not. If it declines to make the measurement, it shows no data from the client.

Note This feature is available to CCX Version 6 clients only if the Foundation service version is 1 or later.

To receive radio measurements, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Note You can also perform a search for a specific client using the NCS Search feature. See the "Using the Search Feature" section on page 2-33 or the "Advanced Search" section on page 2-34 for more information.

Step 3 From the **Test** drop-down list, choose **Radio Measurement**.

Note The Radio Measurement option only appears if the client is Cisco Compatible Extensions v2 (or higher) and is in the associated state (with a valid IP address).

Step 4 Select the check box to indicate if you want to specify beacon measurement, frame measurement, channel load, or noise histogram.

Step 5 Click **Initiate**. The different measurements produce differing results. See the "Radio Measurement Results for a Client" section on page 9-36 for more information.

Note The measurements take about 5 milliseconds to perform. A message from the NCS indicates the progress. If the client chooses not to perform the measurement, that is communicated.

Radio Measurement Results for a Client

Depending on the measurement type requested, the following information might appear:

- Beacon Response
  - Channel—The channel number for this measurement
  - BSSID—6-byte BSSID of the station that sent the beacon or probe response
  - PHY—Physical Medium Type (FH, DSS, OFDM, high rate DSS or ERP)
  - Received Signal Power—The strength of the beacon or probe response frame in dBm
  - Parent TSF—The lower 4 bytes of serving access point TSF value
  - Target TSF—The 8-byte TSF value contained in the beacon or probe response
  - Beacon Interval—The 2-byte beacon interval in the received beacon or probe response
  - Capability information—As found in the beacon or probe response
- Frame Measurement
  - Channel—Channel number for this measurement
  - BSSID—BSSID contained in the MAC header of the data frames received
  - Number of frames—Number of frames received from the transmit address
  - Received Signal Power—The signal strength of 802.11 frames in dBm
- Channel Load
  - Channel—The channel number for this measurement
  - CCA busy fraction—The fractional duration over which CCA indicated the channel was busy during the measurement duration defined as ceiling (255 times the duration the CCA indicated channel was busy divided by measurement duration)
- Noise Histogram
  - Channel—The channel number for this measurement
  - RPI density in each of the eight power ranges

Viewing Client V5 Statistics

To access the Statistics request page, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the **Test** drop-down list, choose **V5 Statistics**.

Note This menu is shown only for CCX v5 and later clients.

Step 4 Click **Go**.

Step 5 Select the desired type of stats (Dot11 Measurement or Security Measurement).

Step 6 Click **Initiate** to initiate the measurements.

Note The duration of measurement is five seconds.

Step 7 Depending on the V5 Statistics request type, the following counters are displayed in the results page:

- Dot11 Measurement
  - Transmitted Fragment Count
  - Multicast Transmitted Frame Count
  - Failed Count
  - Retry Count
  - Multiple Retry Count
  - Frame Duplicate Count
  - Rts Success Count
  - Rts Failure Count
  - Ack Failure Count
  - Received Fragment Count
  - Multicast Received Frame Count
  - FCS Error Count—This counter increments when an FCS error is detected in a received MPDU.
  - Transmitted Frame Count
- Security
  - Pairwise Cipher
  - Tkip ICV Errors
  - Tkip Local Mic Failures
  - Tkip Replays
  - Ccmp Replays
  - Ccmp Decryp Errors
  - Mgmt Stats Tkip ICV Errors
  - Mgmt Stats Tkip Local Mic Failures
  - Mgmt Stats Tkip Replays
  - Mgmt Stats Ccmp Replays
  - Mgmt Stats Ccmp Decrypt Errors

  - Mgmt Stats Tkip MHDR Errors
  - Mgmt Stats Ccmp MHDR Errors
  - Mgmt Stats Broadcast Disassociate Count
  - Mgmt Stats Broadcast Deauthenticate Count
  - Mgmt Stats Broadcast Action Frame Count

Viewing Client Operational Parameters

To view specific client operational parameters, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the **Test** drop-down list, choose **Operational Parameters**.

The following information is displayed:

Operational Parameters:

- Device Name—User-defined name for device.
- Client Type—Client type can be any of the following:
  - laptop(0)
  - pc(1)
  - pda(2)
  - dot11mobilephone(3)
  - dualmodephone(4)
  - wgb(5)
  - scanner(6)
  - tabletpc(7)
  - printer(8)
  - projector(9)
  - videoconfsystem(10)
  - camera(11)
  - gamingsystem(12)
  - dot11deskphone(13)
  - cashregister(14)
  - radiotag(15)
  - rfidsensor(16)
  - server(17)
- SSID—SSID being used by the client.
- IP Address Mode—The IP address mode such as static configuration or DHCP.

- IPv4 Address—IPv4 address assigned to the client.
- IPv4 Subnet Address—IPv4 subnet address assigned to the client.
- IPv6 Address—IPv6 address assigned to the client.
- IPv6 Subnet Address—IPv6 address assigned to the client.
- Default Gateway—The default gateway chosen for the client.
- Operating System—Identifies the operating system that is using the wireless network adaptor.
- Operating System Version—Identifies the version of the operating system that is using the wireless network adaptor.
- WNA Firmware Version—Version of the firmware currently installed on the client.
- Driver Version—
- Enterprise Phone Number—Enterprise phone number for the client.
- Cell Phone Number—Cell phone number for the client.
- Power Save Mode—Displays any of the following power save modes: awake, normal, or maxPower.
- System Name—
- Localization—

Radio Information:

- Radio Type—The following radio types are available:
  - unused(0)
  - fhss(1)
  - dsss(2)
  - irbaseband(3)
  - ofdm(4)
  - hrdss(5)
  - erp(6)
- Radio Channel—Radio channel in use.

DNS/WNS Information:

- DNS Servers—IP address for DNS server.
- WNS Servers—IP address for WNS server.

Security Information:

- Credential Type—Indicates how the credentials are configured for the client.
- Authentication Method—Method of authentication used by the client.
- EAP Method—Method of Extensible Authentication Protocol (EAP) used by the client.
- Encryption Method—Encryption method used by the client.
- Key Management Method—Key management method used by the client.

Viewing Client Profiles

To view specific client profile information, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the More drop-down list, choose **Profiles**.

The following information is displayed:

- Profile Name—List of profile names as hyperlinks. Click to display the profile details.
- SSID—SSID of the WLAN to which the client is associated.

Disabling a Current Client

To disable a current client, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client that you want to disable.

Step 3 Click **Disable**. The Disable Client page appears.

Step 4 Enter a description in the Description text box.

Step 5 Click **OK**.

Note Once a client is disabled, it cannot join any network/ssid on controller(s). To reenable the client, choose **Configure > Controllers >** *IP Address* **> Security > Manually Disabled Clients**, and remove the client entry.

Removing a Current Client

To remove a current client, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client that you want to remove.

Step 3 Choose **Remove**.

Step 4 Click **Remove** to confirm the deletion.

Enabling Mirror Mode

When enabled, mirror mode enables you to duplicate (to another port) all of the traffic originating from or terminating at a single client device or access point.

Note Mirror mode is useful in diagnosing specific network problems but should only be enabled on an unused port as any connections to this port become unresponsive.

To enable mirror mode, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the More drop-down list, choose **Enable Mirror Mode**.

Step 4 Click **Go**.

Viewing a Map (High Resolution) of a Client Recent Location

To display a high-resolution map of the client recent location, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the More drop-down list, choose **Recent Map (High Resolution)**.

Step 4 Click **Go**.

Viewing a Map (High Resolution) of a Client Current Location

To display a high-resolution map of the client present location, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the More drop-down list, choose **Present Map (High Resolution)**.

Step 4 Click **Go**.

Running a Client Sessions Report for the Client

To view the most recent client session report results for this client, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the More drop-down list, choose **Client Sessions Report**.

Step 4 Click **Go**. The Client Session report details display. See the "Client Sessions" section on page 14-47 for more information.

Viewing a Roam Reason Report for the Client

To view the most recent roam report for this client, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the More drop-down list, choose **Roam Reason**.

Step 4 Click **Go**.

This page displays the most recent roam report for the client. Each roam report has the following information:

- New AP MAC address
- Old (previous) AP MAC address
- Previous AP SSID
- Previous AP channel
- Transition time—Time that it took the client to associate to a new access point.
- Roam reason—Reason for the client roam.

Viewing Detecting Access Point Details

To display details of access points that can hear the client including at which signal strength/SNR, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the More drop-down list, choose **Detecting APs**.

Step 4 Click **Go**.

Viewing Client Location History

To display the history of the client location based on RF fingerprinting, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the More drop-down list, choose **Location History**.

Step 4 Click **Go**.

Viewing Voice Metrics for a Client

To view traffic stream metrics for this client, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the More drop-down list, choose **Voice Metrics**.

Step 4 Click **Go**.

The following information appears:

- Time—Time that the statistics were gathered from the access point(s).
- QoS
- AP Ethernet MAC
- Radio
- % PLR (Downlink)—Percentage of packets lost on the downlink (access point to client) during the 90 second interval.
- % PLR (Uplink)—Percentage of packets lost on the uplink (client to access point) during the 90 second interval.
- Avg Queuing Delay (ms) (Uplink)—Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
- % Packets > 40 ms Queuing Delay (Downlink)——Percentage of queuing delay packets greater than 40 ms.
- % Packets 20ms—40ms Queuing Delay (Downlink)—Percentage of queuing delay packets greater than 20 ms.
- Roaming Delay—Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the first packet is received from the new access point after a successful roam.

CHAPTER 10

Using Templates

This chapter describes how to add and apply templates. Templates allow you to set fields that you can then apply to multiple devices without having to reenter the common information. This chapter contains the following sections:

Information About Templates

The Controller Template Launch Pad is a hub for all controller templates. From this Template Launch Pad you can add and apply controller templates, view templates, or make modifications to existing templates. This chapter also includes steps for applying and deleting controller templates and creating or changing access point templates.

Note Template information can be overridden on individual devices.

Accessing the Controller Template Launch Pad

To access the Controller Template Launch Pad, choose **Configure > Controller Template Launch Pad**.

The controller template launch pad provides access to all the NCS templates from a single page. From this page, you can view current controller templates or create and save new templates.

Tip Hover your mouse cursor over the tool tip next to the template type to view more details regarding the template.

Adding Controller Templates

To add a new controller template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **New** beside the template you want to add.

Step 3 Enter the template name.

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

Step 4 Provide a description of the template.

Step 5 Click **Save**.

Deleting Controller Templates

To delete a controller template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click the template type to open its template list page.

Step 3 Select the check box(es) of the template(s) you want to delete.

Step 4 From the Select a command drop-down list, choose **Delete Templates**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion. If this template is applied to controllers, the Remove Template Confirmation page opens and lists all controllers to which this template is currently applied.

Step 7 Select the check box of each controller from which you want to remove the template.

Step 8 Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the template.

Applying Controller Templates

You can apply a controller template directly to a controller or to controllers in a selected configuration group.

To apply a controller template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 From the left sidebar menu, choose the category of templates to apply.

Step 3 Click the template name for the template that you want to apply to the controller.

Step 4 Click **Apply to Controllers** to open the Apply to Controllers page.

Step 5 Select the check box for each controller to which you want to apply the template.

Note To select all controllers, select the check box that appears at the left most corner of the controllers table.

Note Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

Step 6 Choose between applying the template directly to a controller or to all controllers in a selected configuration group.

To apply the template directly to a controller (or controllers), follow these steps:

a. Select the **Apply to controllers selected directly** radio button. The Apply to Controllers page lists the IP address for each available controller along with the controller name and the configuration group name (if applicable).

b. Select the check box for each controller to which you want to apply the template.

Note Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

To apply the template to all controllers in a selected configuration group, follow these steps:

a. Select the **Apply to controllers in the selected Config Groups** radio button. The Apply to Controllers page lists the name of each configuration group along with the mobility group name and the number of controllers included.

b. Select the check box for each configuration group to which you want to apply the template.

Note Configuration groups which have no controllers cannot be selected to apply the templates.

Step 7 You can perform the following additional operations:

- If you select the Save Config to Flash after apply check box, the save config to Flash command is executed after the template is applied successfully.
- If you select the Reboot Controller after apply check box, the controller reboots after the template is successfully applied.

Note This configuration results can be viewed in the Template Results page by enabling the View Save Config / Reboot Results option.

Step 8 Click **Save**.

Note You can apply some templates directly from the Template List page. Select the check box(es) of the template(s) that you want to apply, choose **Apply Templates** from the Select a command drop-down list, and click **Go** to open the Apply to Controllers page. Select the check box(es) of the controllers to which you want to apply this template, and click **OK**.

Configuring Controller Templates

This section contains the following topics:

Configuring System Templates

This section contains the following topics:

Configuring General Templates

To add a general template or make changes to an existing general template, follow these steps:

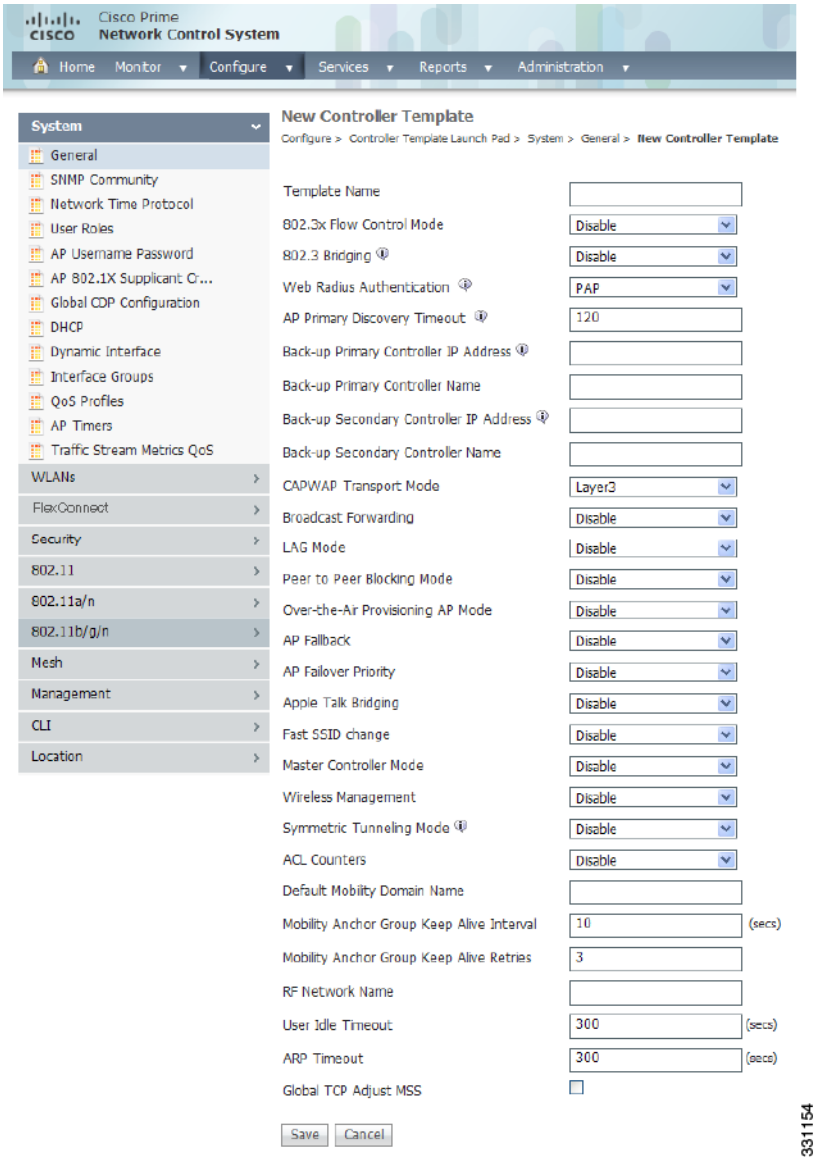
Step 1 Choose **Configure > Controller Template Launch Pad**.

Click **General** or choose **System > General** from the left sidebar menu. The System > General Template page appears, and the number of controllers and virtual domains the template is applied to automatically populates. The last column shows when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page that displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 2 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The General template page appears (see Figure 10-1).

Figure 10-1 System > General Page



Step 3 Use the 802.3x Flow Control Mode drop-down list to enable or disable flow control mode.

Step 4 Use the 802.3x Bridging drop-down list to enable or disable 802.3 bridging.

Note This 802.3 bridging option is not available for 5500 and 2106 series controllers.

Step 5 Use the Web RADIUS Authentication drop-down list to choose the desired Web RADIUS authentication. You can choose to use PAP, CHAP, or MD5-CHAP for authentication between the controller and the client during the user credential exchange.

Step 6 Specify the number of seconds for the AP Primary Discovery Timeout. The default is 120 seconds, and the valid range is 30 to 3600.

Step 7 Specify the Back-up primary and secondary controller details (controller IP address and controller name).

Step 8 Specify Layer 2 or Layer 3 transport mode. When set to Layer 3, the lightweight access point uses IP addresses to communicate with the access points; these IP addresses are collected from a mandatory DHCP server. When set to Layer 2, the lightweight access point uses proprietary code to communicate with the access points.

Note Controllers through Release 5.2 use LWAPP and the new controller release uses CAPWAP.

Step 9 Choose to enable or disable broadcast forwarding. The default is disabled.

Step 10 Choose **Enable** or **Disable** from the LAG Mode drop-down list. Link aggregation allows you to reduce the number of IP addresses needed to configure the ports on your controller by grouping all the physical ports and creating a link aggregation group (LAG).

If LAG is enabled on a controller, any dynamic interfaces that you have created are deleted to prevent configuration inconsistencies in the interface database. When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect.

Note Interfaces cannot be created with the Dynamic AP Manager flag set. Also, you cannot create more than one LAG on a controller.

Step 11 Choose to enable or disable peer-to-peer blocking mode. If you choose Disable, any same-subnet clients communicate through the controller. If you choose Enable, any same-subnet clients communicate through a higher-level router.

Step 12 From the Over Air AP Provision Mode drop-down list, choose **enable** or **disable**.

Step 13 From the AP Fallback drop-down list, choose **enable** or **disable**. Enabling fallback causes an access point that lost a primary controller connection to automatically return to service when the primary controller returns.

Step 14 When a controller fails, the backup controller configured for the access point suddenly receives a number of discovery and join requests. This might cause the controller to reach a saturation point and reject some of the access points. By assigning priority to an access point, you have some control over which access points are rejected. In a failover situation when the backup controller is saturated, the higher priority access points can join the backup controller if the lower priority access points are disjoined. Choose **enable** from the AP Failover Priority drop-down list if you want to allow this capability.

Step 15 Choose to enable or disable AppleTalk bridging.

Note This AppleTalk bridging option is not available on 5500 series controllers.

Step 16 Choose to enable or disable the Fast SSID Change option. If the option is enabled, the client connects instantly to the controller between SSIDs without having much loss of connectivity. Normally, each client is connected to a particular WLAN identified by the SSID. If the client moves out of reach of the connected access point, the client has to reconnect to the controller using a different access point. This normal process consumes some time as the DHCP (Dynamic Host Configuration Protocol) server has to assign an IP address to the client.

Step 17 Because the master controller is normally not used in a deployed network, the master controller setting is automatically disabled upon reboot or operating system code upgrade. You might want to enable the controller as the master controller from the Master Controller Mode drop-down list.

Step 18 Choose to enable or disable access to the controller management interface from wireless clients. Because of IPsec operation, management via wireless is only available to operators logging in across WPA or Static WEP. Wireless management is not available to clients attempting to log in via an IPsec WLAN.

Step 19 Choose to enable or disable symmetric tunneling mode. With symmetric mobility tunneling, the controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. The client traffic on the wired network is directly routed by the foreign controller. If a router has Reverse Path Forwarding (RPF) enabled (which provides additional checks on incoming packets), the communication is blocked. Symmetric mobility tunneling allows the client traffic to reach the controller designated as the anchor, even with RPF enabled.

Note All controllers in a mobility group should have the same symmetric tunneling mode.

Note For symmetric tunneling to take effect, you must reboot.

Step 20 Use the ACL Counters drop-down list to enable or disable ACL counters. The values per ACL rule can be viewed for each controller.

Step 21 Enter the operator-defined RF mobility group name in the Default Mobility Domain Name text box.

Step 22 At the Mobility Anchor Group Keep Alive Interval, determine the delay between tries for clients attempting to join another access point. With this guest tunneling N+1 redundancy feature, the time it takes for a client to join another access point following a controller failure is decreased because a failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

Note When you hover your mouse cursor over the field, the valid range of values appear.

Step 23 At the Mobility Anchor Group Keep Alive Retries, specify the number of queries to anchor before the client declares it unreachable.

Step 24 Enter the RF network group name between 8 and 19 characters. Radio Resource Management (RRM) neighbor packets are distributed among access points within an RF network group. The Cisco access points only accept RRM neighbor packets sent with this RF network name. The RRM neighbor packets sent with different RF network names are dropped.

Step 25 Specify the time out for idle clients. The factory default is 300 seconds. When the timeout expires, the client loses authentication, briefly disassociates from the access point, reassociates, and re-authenticates.

Step 26 Specify the timeout in seconds for the address resolution protocol. The factory default is 300 seconds.

Step 27 Select the **Global TCP Adjust MMS** check box to start checking the TCP packets originating from the client, for the TCP SYN/ TCP ACK packets and MSS value and reset it to the configured value on the upstream and downstream side.

Step 28 Choose **enable** or **disable** Web Auth Proxy Redirect Mode if a manual proxy configuration is configured on the browser of the client; all web traffic going out from the client is destined for the PROXY IP and PORT configured on the browser.

Step 29 Enter the Web Auth Proxy Redirect Port. The default ports are 8080 and 3128. The range is 0 to 65535.

Step 30 Enter the AP Retransmit Count and Intervals. The AP Retransmit Count default value is 5 and the range is from 3 to 8. The AP Retransmit Interval default value is 3. The range is 2 to 5.

Step 31 Click **Save**.

Configuring SNMP Community Controller Templates

Create or modify a template for configuring SNMP communities on controllers. Communities can have read-only or read-write privileges using SNMP v1, v2, or v3.

To add a new template with SNMP community information for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **New** beside the template you want to add.

Step 3 Configure the following fields:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Community Name
- Confirm Community Name—Retype the community name.
- IP Address—The IP address of the server.
- Netmask
- Access Mode—Choose **Read Only** or **Read Write** from the drop-down list.
  - Read Only—Cannot be edited.
  - Read Write—Can be edited.
- Admin Status—Select the check box to enable this template and also to enable the Update Discover Community option.
- Update Discover Community—Select the check box to update the SNMP version as v2. This updates the Read/Write Community as the template community name for the applied controllers.

Note If the Access Mode option is configured as Read Only, then the NCS has only read access to the controller after applying this template.

Step 4 Click **Save**. Once saved, the template appears in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 10-2 for more information.

Note If a template is applied successfully and the Update Discover Community option is enabled, then the applied community name is updated in the NCS database for that applied controller. Also, the NCS uses that community name for further communication with that controller.

Configuring an NTP Server Template

Note NTP is used to synchronize computer clocks on the Internet.

To add an NTP template or make modifications to an existing NTP template, follow these steps:

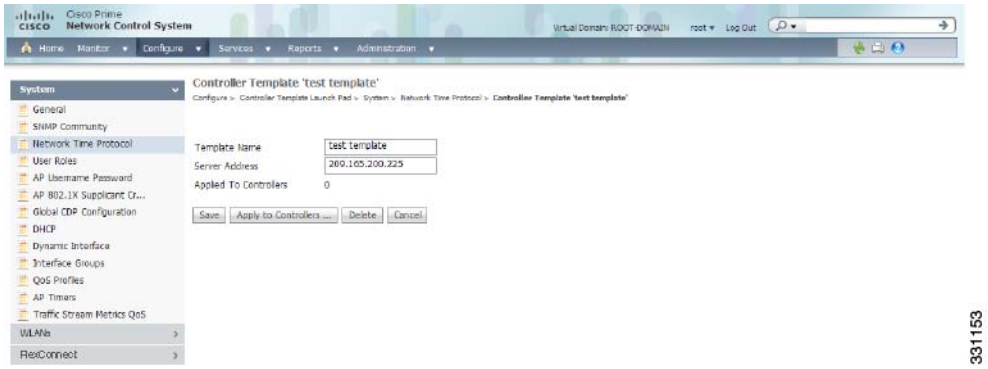
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Network Time Protocol** or choose **System > Network Time Protocol** from the left sidebar menu. The System > NTP Server Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens the Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens to an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Network Time Protocol template page appears (see Figure 10-2).

Figure 10-2 NTP Servers Template



Step 4 Enter the NTP server IP address.

Step 5 Click **Save**.

Configuring User Roles Controller Templates

This section describes how to create or modify a template for configuring user roles. User roles determine how much bandwidth the network can use. Four QoS levels (Platinum, Bronze, Gold, and Silver) are available for the bandwidth distribution to Guest Users. Guest Users are associated with predefined roles (Contractor, Customer, Partner, Vendor, Visitor, Other) with respective bandwidth configured by the Admin. These roles can be applied when adding a new Guest User. See the "Configuring a Guest User Template" section on page 10-60 for more information on adding Guest Users.

To add a new template with User Roles information for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **New** beside the template you want to add.

Step 3 Configure the following fields:

- Role Name
- Average Data Rate—The average data rate for non-UDP (User Datagram Protocol) traffic.
- Burst Data Rate—The peak data rate for non-UDP traffic.
- Average Real-time Rate—The average data rate for UDP traffic.
- Burst Real-time Rate—The peak data rate for UDP traffic.

Step 4 Click **Save**. Once saved, the template displays in the Template List page. From the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 10-2 for more information.

Configuring AP Username Password Controller Templates

Create or modify a template for setting an access point username and password. All access points inherit the password as they join the controller and these credentials are used to log into the access point via the console or Telnet/SSH.

Note See the "Configuring a Global Access Point Password" section on page 8-60 for more information regarding global passwords.

The AP Username Password page enables you to set a global password that all access points inherit as they join a controller. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis. See the "Configuring AP Configuration Templates" section on page 10-137 to see where the global password is displayed and how it can be overridden on a per-access point basis.

Also, in controller software Release 5.0, after an access point joins the controller, the access point enables console port security and you are prompted for your username and password whenever you log into the access point console port. When you log in, you are in non-privileged mode and you must enter the enable password to use the privileged mode.

To add a new template with AP Username Password information for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **New** beside the template you want to add.

Step 3 Configure the following fields:

- AP Username—Type the username that you want to be inherited by all access point that join the controller.
- AP Password—Type the password that you want to be inherited by all access point that join the controller.
- Confirm Password—Retype the access point password.
- Enable Password

Note For Cisco IOS access points, you must also enter and confirm an enable password.

- Confirm Enable Password

Step 4 Click **Save**. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 10-2 for more information.

Note See the "Configuring a Global Access Point Password" section on page 8-60 for more information regarding global passwords.

Configuring AP 802.1X Supplicant Credentials

You can configure 802.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning. You can set global authentication settings that all access points inherit as they join the controller. All access points that are currently joined to the controller and any that join in the future are included.

To add or modify an existing AP 802.1X Supplicant Credentials template, follow these steps:

Note If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point. See the "Configuring Access Points" section on page 8-161 for more information.

Step 1 Choose **Configure > Controller Templates Launch Pad**.

Step 2 Click **AP 802.1X Supplicant Credentials** or choose **System > AP 802.1X Supplicant Credentials** from the left sidebar menu. The AP 802.1X Supplicant Credentials Templates page displays all currently saved AP 802.1X Supplicant Credentials templates. It also displays the number of controllers and virtual domains to which each template is applied.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 Click a template name to open the Controller Template list page. From there, you can edit the current template fields.

Step 4 Click **Save**.

Configuring a Global CDP Configuration Template

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

Note CDP is enabled on the Ethernet and radio ports of the bridge by default.

To configure a Global CDP Configuration template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Global CDP Configuration** or choose **System > Global CDP Configuration** from the left sidebar menu. The Global CDP Configuration Templates page displays all currently saved Global CDP Configuration templates.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Global CDP Configuration template page appears.

Step 4 Enter the new CDP template name.

Step 5 In the Global CDP group box of the page, configure the following fields:

- CDP on controller—Choose enable or disable CDP on the controller.

  Note This configuration cannot be applied on WiSM2 controllers.

- Global CDP on APs—Choose to enable or disable CDP on the access points.
- Refresh-time Interval (seconds)—At the Refresh Time Interval field, enter the time in seconds at which CDP messages are generated. The default is 60.
- Holdtime (seconds)—Enter the time in seconds before the CDP neighbor entry expires. The default is 180.
- CDP Advertisement Version—Enter which version of the CDP protocol to use. The default is v1.

Step 6 In the CDP for Ethernet Interfaces group box of the page, select the slots of Ethernet interfaces for which you want to enable CDP.

Note CDP for Ethernet Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 7 In the CDP for Radio Interfaces group box of the page, select the slots of Radio interfaces for which you want to enable CDP.

Note CDP for Radio Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 8 Click **Save**.

Note The Global Interface CDP configuration is applied only to the APs for which the CDP is enabled at AP level.

Configuring DHCP Templates

To add a DHCP template or make modifications to an existing DHCP template, follow these steps:

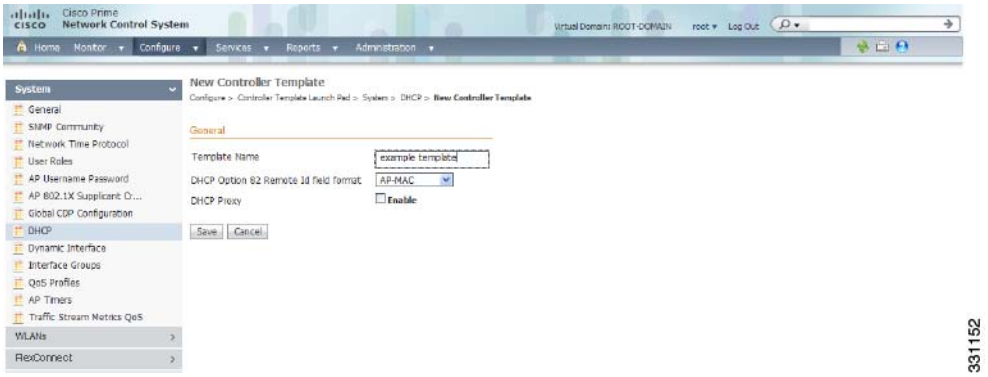
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **DHCP** or choose **System > DHCP** from the left sidebar menu. The System > DHCP Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The DHCP template page appears (see Figure 10-3).

Figure 10-3 DHCP Template Page



Step 4 You can enable or disable DHCP proxy on a global basis rather than on a WLAN basis. When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. At least one DHCP server must be configured on either the interface associated with the WLAN or on the WLAN itself. DHCP proxy is enabled by default.

Step 5 Enter the DHCP Timeou,t in seconds, after which the DHCP request times out. The default setting is 5. Allowed values range from 5 to 120 seconds.

Note DHCP Timeout is applicable for Controller Release 7.0.114.74 and later.

Step 6 Click **Save**.

Configuring Dynamic Interface Templates

To add a dynamic interface template or make modifications to an existing interface configuration, follow these steps:

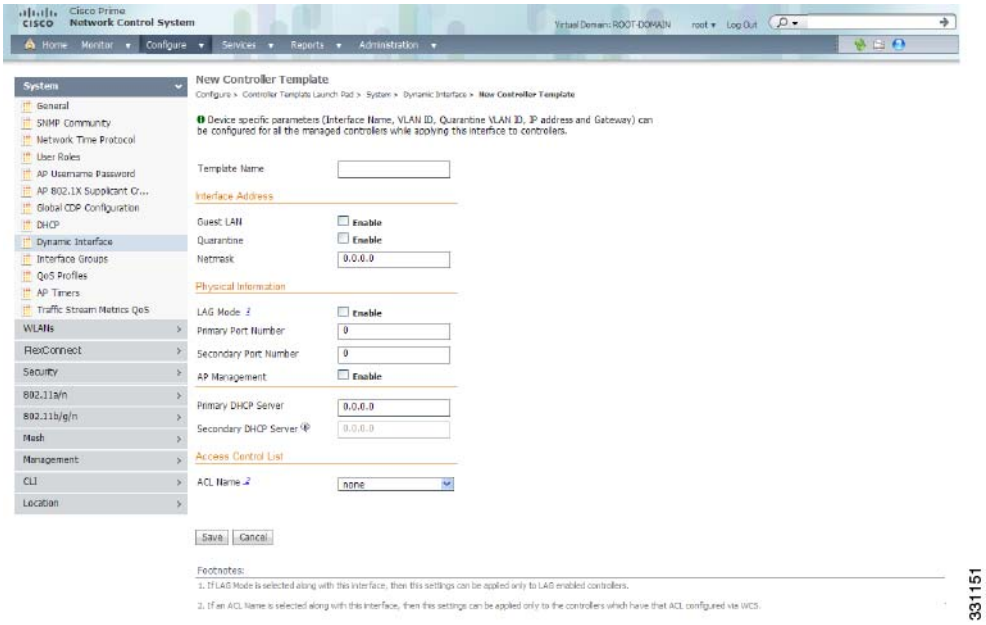
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Dynamic Interface** or choose **System > Dynamic Interface** from the left sidebar menu. The System > Dynamic Interface Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Dynamic Interface template page appears (see Figure 10-4).

Figure 10-4 Dynamic Interface Template



Step 4 Select the **Guest LAN** check box to mark the interface as wired.

Step 5 Enter the net mask address of the interface.

Step 6 Enter the port currently used by the interface.

Step 7 Enter a secondary port to be used by the interface when the primary port is down. When the primary port is reactivated, the Cisco 4400 Series Wireless LAN controller transfers the interfaces back to the primary port.

Note Primary and secondary port numbers are present only in the Cisco 4400 Series Wireless LAN controllers.

Step 8 Enter the IP address of the primary DHCP server.

Step 9 Enter the IP address of the secondary DHCP server.

Step 10 From the ACL Name drop-down list, choose a name from the list of defined names.

Step 11 From the Add Format Type drop-down list in the Add Interface Format Type group box, choose either **Device Info** or **File**. If you choose device info, you must configure the device-specific fields for each controller. If you choose File, you must configure CSV device-specific fields (Interface Name, VLAN Identifier, Quarantine VLAN Identifier, IP Address, and Gateway) for all the managed controllers specified in the CSV file (see Table 10-1). If you choose Device Info, continue to Step 12.

The sample CSV files are as follows.

Table 10-1 Sample CSV Files

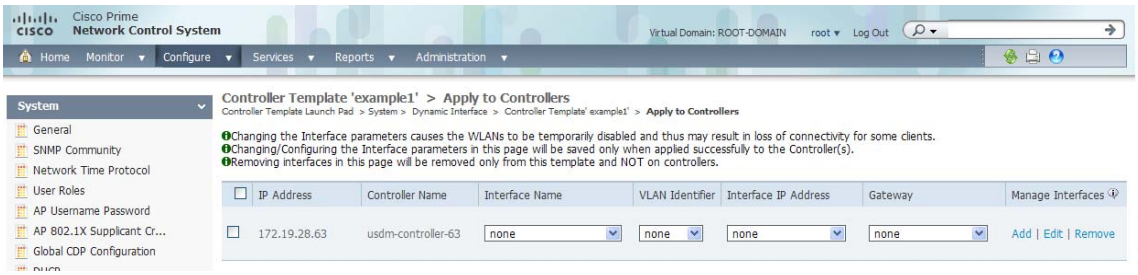
ip_address	interface_name	vlan_id	quarantine_ vlan_id	interface_ ip_address	gateway
209.165.200.224	dyn-1	1	2	209.165.200.228	209.165.200.229
209.165.200.225	interface-1	4	2	209.165.200.230	209.165.200.231
209.165.200.226	interface-2	5	3	209.165.200.232	209.165.200.233
209.165.200.227	dyna-2	2	3	209.165.200.234	209.165.200.235

The first row of the CSV file is used to describe the columns included. The CSV files can contain the following fields:

- ip_address
- interface_name
- vlan_id
- quarantine_vlan_id
- interface_ip_address
- gateway

Step 12 If you choose Apply to Controllers, you advance to the Apply To page where you can configure device-specific fields for each controller (see Figure 10-5).

Figure 10-5 Apply To Page



Step 13 Use the **Add** and **Remove** options to configure device specific fields for each controllers. If you click **Edit**, a dialog box appears with the current parameter input.

Step 14 Make the necessary changes in the dialog box, and click **OK**.

Note If you change the interface fields, the WLANs are temporarily disabled, therefore you might lose connectivity for some clients. Any changes to the interface fields are saved only after you successfully apply them to the controller(s).

Note If you remove an interface here, it is removed only from this template and not from the controllers.

Applying a Dynamic Interface Template to Controllers

To apply a Dynamic Interface template to a controller, follow these steps:

Step 1 In the Dynamic Interface controller template page, click **Apply to Controllers**.

Step 2 Use the Manage Interfaces options to configure device-specific fields:

- Add—Click **Add** to open the Add Interface dialog box. Enter an interface name, VLAN identifier, IP address, and gateway. When all fields are entered, click **Done**.
- Edit—Click **Edit** to make changes to current interfaces.
- Remove—Click **Remove** to delete a current interface.

Step 3 Select a check box for each controller to which you want to apply this template.

Step 4 Click **Apply**.

Note Changing the Interface fields causes the WLANs to be temporarily disabled and might result in loss of connectivity for some clients.

Note Interface field changes or configurations made on this page are saved only when applied successfully to the controller(s).

Note Interfaces removed from this page are removed only from this template and not from controllers.

Note See the "Configuring Dynamic Interface Templates" section on page 10-15 for more information on Dynamic Interface controller templates.

Configuring QoS Templates

To modify the quality of service (QoS) profiles, follow these steps:

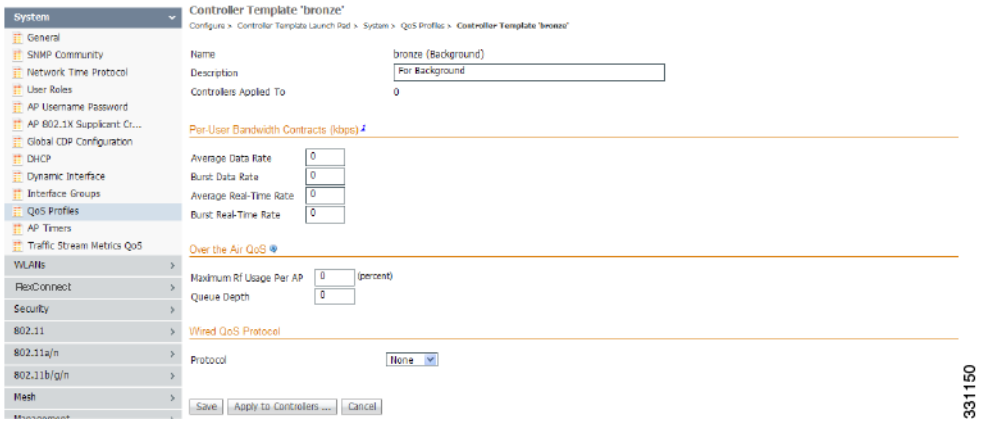
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **QoS Profiles** or choose **System > QoS Profiles** from the left sidebar menu. The System > QoS Profiles page appears. The number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to edit the bronze, gold, platinum, or silver QoS profile, click in the Name column for the profile you want to edit. The Edit QoS Profile Template page appears (see Figure 10-6).

Figure 10-6 Edit QoS Profile Template Page



Step 4 Set the following values in the Per-User Bandwidth Contracts group box. All have a default of 0 or Off.

- Average Data Rate—The average data rate for non-UDP traffic.
- Burst Data Rate—The peak data rate for non-UDP traffic.
- Average Real-time Rate—The average data rate for UDP traffic.
- Burst Real-time Rate—The peak data rate for UDP traffic.

Step 5 Set the following values in the Over-the-Air QoS group box.

- Maximum QoS RF Usage per AP - The maximum air bandwidth available to clients. The default is 100%.
- QoS Queue Depth - The depth of queue for a class of client. The packets with a greater value are dropped at the access point.

Note The Air QoS configurations are applicable for controller Release 7.0 and earlier.

Step 6 Set the following values in the Wired QoS Protocol group box.

- Wired QoS Protocol - Choose **802.1P** to activate 802.1P priority tags or **None** to deactivate 802.1P priority flags.
- 802.1P Tag - Choose **802.1P priority tag** for a wired connection from 0 to 7. This tag is used for traffic and CAPWAP packets.

Step 7 Click **Save**.

Configuring AP Timers Templates

Some advanced timer configuration for FlexConnect and local mode is available for the controller on the NCS.

To configure a template for AP timers, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **AP Timers** or choose **System > AP Timers** from the left sidebar menu. The System > AP Timers page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

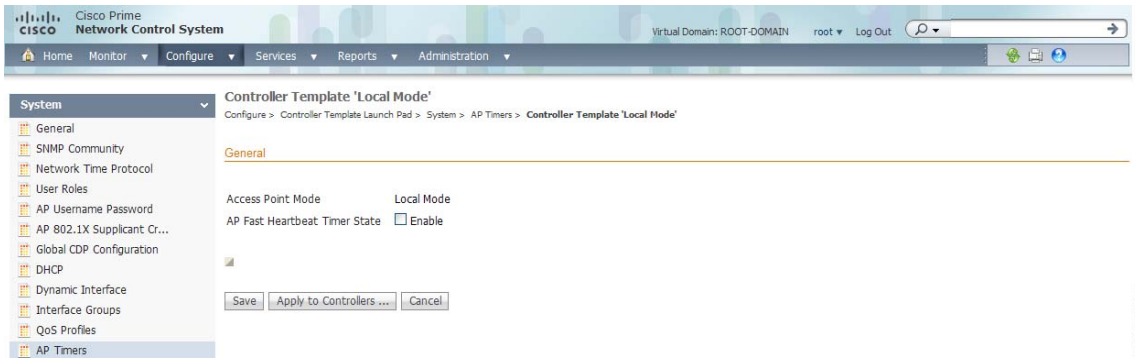
The values in the Access Point Mode column are links. When you click a link, the Controller Template *access point mode* page appears. The Access Point Mode is automatically populated (see Figure 10-7).

Step 3 Select the **AP Fast Heartbeat Timer State** check box to enable AP Fast Heartbeat Timeout.

Step 4 Enter an AP Fast Heartbeat Timeout value. The valid range is 1 to 15 seconds. The default is 10 seconds. The recommended timeout values are:

- 10 to 15 seconds for 7500 series controllers.
- 10 to 15 seconds for 5500 series controllers Release 7.0.98.0 and earlier.
- 1 to 10 seconds for 5500 series controllers Release 7.0.98.0 and later.
- 1 to10 seconds for other controllers.

Figure 10-7 AP Timers Page



Step 5 Click **Save**.

Configuring an Interface Group Template

The interface group template page allows you to select list of interfaces and form a group.

Note You cannot create interfaces using this page.

To configure an interface group template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Interface Groups** or choose **System > Interface Groups** from the left sidebar menu. The System > Interface Groups page appears.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The New Controller template page appears.

Step 4 Specify the following details:

- Name—Interface Group name.
- Description(optional)—A more detailed description of the interface group.
- Quarantine—Indicates the type of interfaces that can be added to an interface group. If this option is enabled, you can add interfaces with quarantine VLAN ID set. If this options is disabled, you can add interfaces with quarantine VLAN ID not set.

Step 5 Selected Controllers/Interfaces that you want to add to the group.

Step 6 Click **Save**.

Configuring a Traffic Stream Metrics QoS Template

Traffic stream metrics are a series of statistics about VoIP over your wireless LAN and informs you of the QoS of the wireless LAN. These statistics are different than the end-to-end statistics provided by VoIP systems. End-to-end statistics provide information on packet loss and latency covering all the links comprising the call path. However, traffic stream metrics are statistics for only the WLAN segment of the call. Because of this, system administrators can quickly determine whether audio problems are being caused by the WLAN or by other network elements participating in a call. By observing which access points have impaired QoS, system administrators can quickly determine the physical area where the problem is occurring. This is important when lack of radio coverage or excessive interference is the root problem.

Four QoS values (packet latency, packet jitter, packet loss, and roaming time), which can affect the audio quality of voice calls, are monitored. All the wireless LAN components participate in this process. Access points and clients measure the metrics, access points collect the measurements and then send them to the controller. The access points update the controller with traffic stream metric information every 90 seconds, and 10 minutes of data is stored at one time. The NCS queries the controller for the metrics and displays them in the Traffic Stream Metrics QoS Status. These metrics are compared to threshold values to determine their status level and if any of the statistics are displaying a status level of fair (yellow) or degraded (red), the administrator investigates the QoS of the wireless LAN.

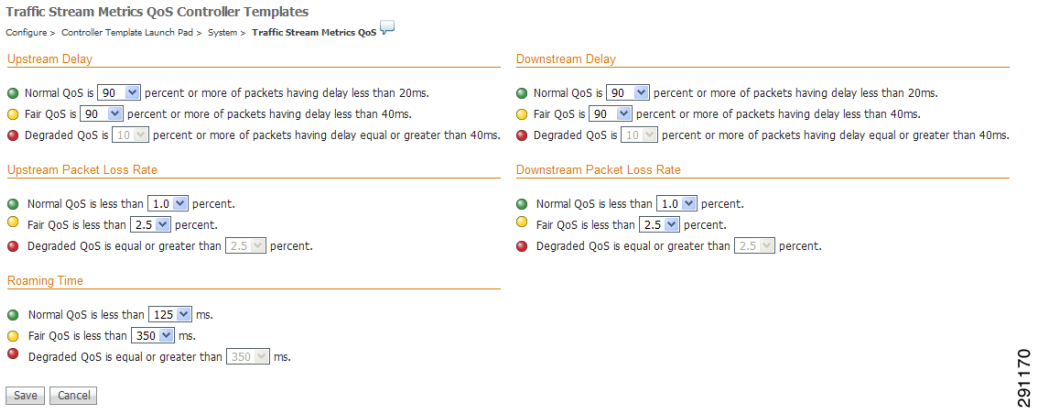
For the access points to collect measurement values, traffic stream metrics must be enabled on the controller.

To configure a Traffic Stream Metrics QoS template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Traffic Stream Metrics QoS** or choose **System > Traffic Stream Metrics QoS** from the left sidebar menu. The Traffic Stream Metrics QoS Controller Templates page appears (see Figure 10-8).

Figure 10-8 Traffic Stream Metrics QoS Status Template



The Traffic Stream Metrics QoS Controller Configuration page shows several QoS values. An administrator can monitor voice and video quality of the following:

- Upstream delay
- Upstream packet loss rate
- Roaming time
- Downstream packet loss rate
- Downstream delay

Packet Loss Rate (PLR) affects the intelligibility of voice. Packet delay can affect both the intelligibility and conversational quality of the connection. Excessive roaming time produces undesired gaps in audio.

There are three levels of measurement:

- Normal: Normal QoS (green)
- Fair: Fair QoS (yellow)
- Degraded: Degraded QoS (red)

System administrators should employ some judgement when setting the green, yellow, and red alarm levels. Some factors to consider are:

- Environmental factors including interference and radio coverage which can affect PLR.
- End-user expectations and system administrator requirements for audio quality on mobile devices (lower audio quality can permit greater PLR).
- Different codec types used by the phones have different tolerance for packet loss.
- Not all calls are mobile-to-mobile; therefore, some have less stringent PLR requirements for the wireless LAN.

Configuring WLAN Templates

This section contains the following topics:

- Configuring WLAN AP Groups Templates, page 10-39

Configuring WLAN Templates

WLAN templates allow you to define various WLAN profiles for application to different controllers.

You can configure multiple WLANs with the same SSID. This feature enables you to assign different Layer 2 security policies within the same wireless LAN. Unlike previous release where profile name was used as the unique identifier, the template name is now the unique identifier with software release 5.1.

These restrictions apply when configuring multiple WLANs with the same SSID:

- WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in the beacons and probes. These are the available Layer 2 security policies:
  - None (open WLAN)
  - Static WEP or 802.1
  - CKIP
  - WPA/WPA2
- Broadcast SSID must be enabled on the WLANs that share an SSID so that the access points can generate probe responses for these WLANs.
- FlexConnect access points do not support multiple SSIDs.

To add a WLAN template or make modifications to an existing WLAN template, follow these steps:

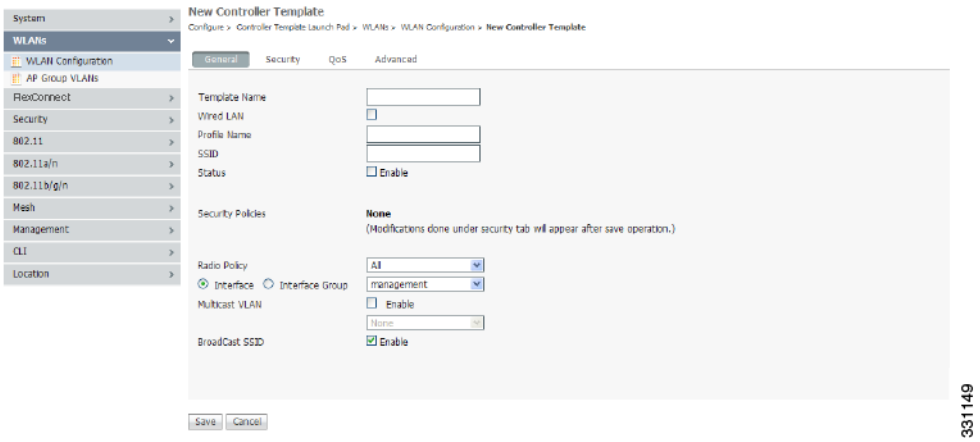
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **WLAN** or choose **WLANs > WLAN Configuration** from the left sidebar menu. The WLAN template page appears with a summary of all existing defined WLANs. The following information headings are used to define the WLANs listed in the WLAN Template General page:

- Template Name—The user-defined name of the template. Clicking the name displays fields for this template.
- Profile Name—User-defined profile name used to distinguish WLANs with the same SSID.
- SSID—Displays the name of the WLAN.
- WLAN/Guest LAN—Determines if guest LAN or WLAN.
- Security Policies—Indicates what security policy is chosen. None indicates no 802.1X.
- WLAN Status—Determines whether the WLAN is enabled or not.
- Applied to Controllers—The number of controllers the WLAN template is applied to. The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status.
- Applied to Virtual Domains—The number of virtual domains the WLAN template is applied to. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.
- Last Saved At—Indicates when the template was last saved.

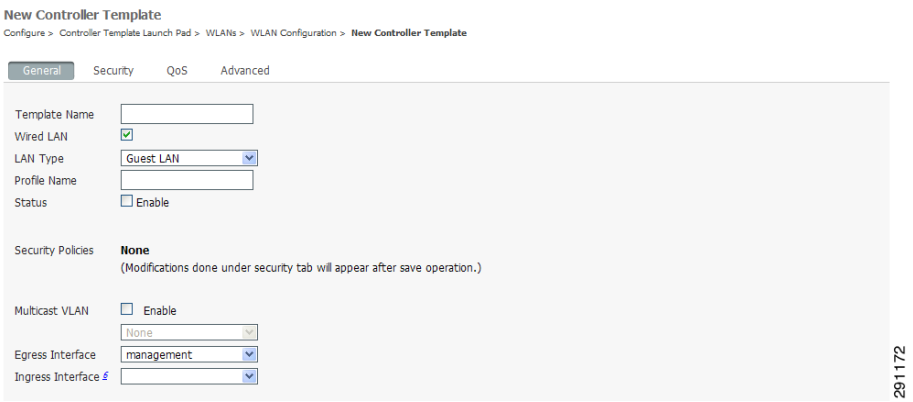
Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The WLAN template page appears (see Figure 10-9).

Figure 10-9 WLAN Template



Step 4 Select the **Wired LAN** check box to indicate whether or not this WLAN is a wired LAN.

Figure 10-10 WLAN Template



Note Specify if you want guest users to have wired guest access from an Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room and accounts are added to the network using the Lobby Ambassador portal. (See the "Creating Guest User Accounts" section on page 6-10).

Note The Egress or Ingress interface configurations are applicable for Wired LAN only.

Step 5 Use the **Type** drop-down list to select the type of the wired LAN.

- Guest LAN—Indicates that this wired LAN is a Guest LAN.

Note If you selected the Guest LAN option, you need to select an Ingress interface which has not already been assigned to any Guest LAN.

- Remote LAN—Indicates that this wired LAN is a Remote LAN.

Step 6 Enter a name in the Profile Name text box that identifies the WLAN or the guest LAN. Do not use any spaces in the name entered.

Step 7 Enter the name of the WLAN SSID. An SSID is not required for a guest LAN.

WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in the beacons and probes.

Step 8 Select the **Enable** check box for the Status field.

Step 9 Use the Radio Policy drop-down list to set the WLAN policy to apply to All (802.11a/b/g/n), 802.11a only, 802.11g only, 802.11b/g only, or 802.11a/g only.

Step 10 Use the Interface/Interface Group drop-down list to choose the available names of interfaces created by the Controller > Interfaces module.

Step 11 From the Egress Interface drop-down list, choose the Egress interface that you created in the "Creating an Egress Interface" section on page 8-49. This provides a path out of the controller for wired guest client traffic.

Step 12 From the Ingress Interface drop-down list, choose the Ingress interface that you created in the "Creating an Ingress Interface" section on page 8-49. The provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 13 Select the **Enable** check box to enable the multicast VLAN feature.

Step 14 From the Multicast VLAN Interface drop-down list, choose the appropriate interface name. This list is automatically populated when you enable the multicast VLAN feature.

Step 15 Click **Broadcast SSID** to activate SSID broadcasts for this WLAN.

Step 16 Click **Save**.

Step 17 To further configure the WLAN template, choose from the following:

- Click the **Security** tab to establish which AAA can override the default servers on this WLAN and to establish the security mode for Layer 2 and 3. Continue to the "Security Tab" section on page 10-25.
- Click the **QoS** tab to establish which quality of service is expected for this WLAN. Continue to the "QoS Tab" section on page 10-33.
- Click the **Advanced** tab to configure any other details about the WLAN, such as DHCP assignments and management frame protection. Continue to the "Advanced Tab" section on page 10-34.

Security Tab

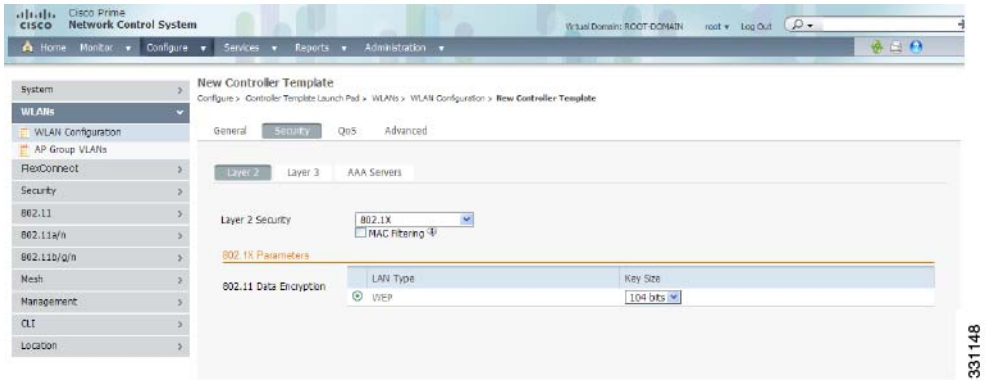
After choosing Security, you have an additional three tabs: Layer 2, Layer 3, and AAA Servers.

Layer 2 Tab

When you click the Layer 2 tab, the Layer 2 tab appears (see Figure 10-11).

Note The tab contains different views depending on what option is chosen in the Layer 2 Security drop-down list.

Figure 10-11 Layer 2 Tab



To configure the Layer 2 tab, follow these steps:

Step 1 Use the Layer 2 Security drop-down list to choose None, 802.1X, Static WEP, Static WEP-802.1X, WPA + WPA2, or CKIP as described in Table 10-2.

Table 10-2 Layer 2 Security Options

Field	Description
None	No Layer 2 security selected. • FT Enable—Select the check box to enable Fast Transition (FT) between access points. **Note** Fast transition is not supported with FlexConnect mode. – Over the DS—Select the check box to enable or disable the fast transition over a distributed system. – Reassociation Timeout—Time in seconds after which fast transition reassociation times out. The default is 20 seconds, and the valid range is 1 to 100. **Note** To enable Over the DS or Reassociation Timeout, you must enable fast transition.
802.1X	WEP 802.1X data encryption type (Note 1): 40/64 bit key. 104 bit key. 152 bit key.

Table 10-2 Layer 2 Security Options (continued)

Field	Description
Static WEP	Static WEP encryption fields: Key sizes: Not set, 40/64, 104, and 152 bit key sizes. Key Index: 1 to 4 (Note 2). Encryption Key: Encryption key required. Key Format: ASCII or HEX. Allowed Shared Key Authentication—Select the check box to enable shared key authentication. **Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and the NCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.
Static WEP-802.1X	Use this setting to enable both Static WEP and 802.1X policies. If this option is selected, static WEP and 802.1X fields are displayed at the bottom of the page. Static WEP encryption fields: Key sizes: Not set, 40/64, 104, and 152 bit key sizes. Key index: 1 to 4 (Note 2). Encryption Key: Enter encryption key. Key Format: ASCII or HEX. Allowed Shared Key Authentication—Select the check box to enable. 802.1 Data Encryption: 40/64 bit key, 104 bit key, 152 bit key.

Table 10-2 Layer 2 Security Options (continued)

Field	Description
WPA+WPA2	Use this setting to enable WPA, WPA2, or both. WPA enables Wi-Fi Protected Access with TKIP-MIC Data Encryption or AES. When WPA+WPA2 is selected, you can use Cisco Centralized Key Management (CCKM) authentication key management, which allows fast exchange when a client roams from one access point to another. When WPA+WPA2 is selected as the Layer 2 security policy and preshared key is enabled, neither CCKM nor 802.1X can be enabled; although, both CCKM and 802.1X can be enabled at the same time. • Mac Filtering—Enables MAC address filtering. **Note** Mac Filtering and Max-Clients are not supported with FlexConnect local authentication. • FT Enable—Select the check box to enable fast transition between access points. **Note** Fast transition is not supported with FlexConnect mode. – Over the DS—Select the check box to enable the fast transition over a distributed system. – Reassociation Timeout—Time in seconds after which fast transition reassociation times out. The default is 20 seconds, and the valid range is 1 to 100. **Note** To enable Over the DS or Reassociation Timeout, enable fast transition. WPA+WPA2 parameters: • WPA1—Select the check box to enable WPA1. • WPA2—Select the check box to enable WPA2. Authentication Key Management: • FT802.1X—Select the check box to enable FT802.1X. • 802.1X—Select the check box to enable 802.1X. • CCKM—Select the check box to enable CCKM. • PSK—Select the check box to enable PSK. • FTPSK—Select the check box to enable FTPSK. **Note** Enable WPA2 and fast transition to set FT802.1X or FTPSK.

Table 10-2 Layer 2 Security Options (continued)

Field	Description
CKIP	Cisco Key Integrity Protocol (CKIP). A Cisco access point advertises support for CKIP in beacon and probe response packets. CKIP can be configured only when Aironet IE is enabled on the WLAN. **Note** CKIP is not supported on 10xx APs. When selected, these CKIP fields are displayed. Key size: Not set, 40, or 104. Key Index: 1 to 4 Encryption Key: Specify encryption key. Key Format: ASCII or HEX. **Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and the NCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device. MMH Mode: Select the check box to enable. Key Permutation: Select the check box to enable.

Step 2 Select the **MAC Filtering** check box if you want to filter clients by MAC address.

Note The ability to join a controller without specification within a MAC filter list is only supported on mesh access points.

Note For releases prior to 4.1.82.0, mesh access points do not join the controller unless they are defined in the MAC filter list.

You might want to disable the MAC filter list to allow newly added access points to join the controller. Before enabling the MAC filter list again, you should enter the MAC addresses of the new access points.

Step 3 Choose the desired type of authentication key management. The choices are 802.1X, CCKM, or PSK.

Note If you choose PSK, you must enter the shared key and type (ASCII or hexadecimal).

Note Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and the NCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.

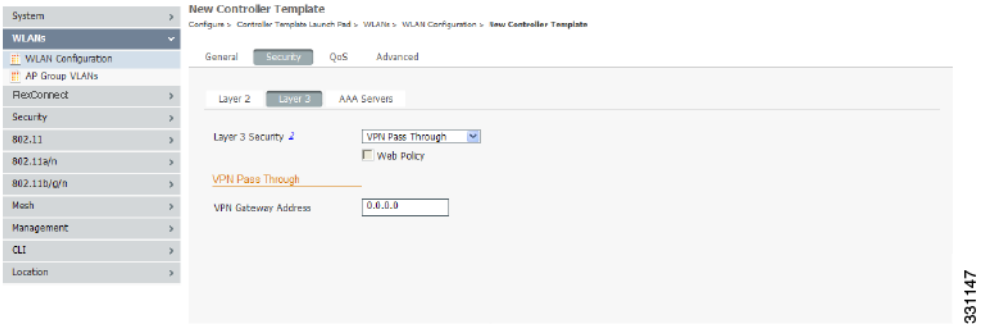
Step 4 Click **Save**.

Layer 3 Tab

When you click the Layer 3 tab, the Layer 3 tab appears (see Figure 10-12).

Note The tab contains different views depending on the option you chose from the Layer 3 Security drop-down list.

Figure 10-12 Layer 3 Tab



To configure the Layer 3 tab, follow these steps:

Step 1 Use the Layer 3 security drop-down list to choose between None and VPN Pass Through. The page fields change according to the selection you make. If you choose VPN pass through, you must enter the VPN gateway address.

Note The VPN passthrough option is not available for the 2106 or 5500 series controllers.

Step 2 You can modify the default static WEP (web authentication) or assign specific web authentication (login, logout, login failure) pages and the server source.

a. To change the static WEP to passthrough, select the **Web Policy** check box and choose the Passthrough option from the drop-down list. This option allows users to access the network without entering a username or password.

   An Email Input check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

b. Choose the **WebAuth on MAC Filter Failure** option so that when clients fail on MAC filter, they are automatically switched to webAuth.

Note The WebAuth on Mac Filter Failure option works only when the Layer 2 Mac Filtering option is enabled.

c. To specify custom web authentication pages, unselect the **Global WebAuth Configuration Enable** check box.

1. When the Web Auth Type drop-down list appears, choose one of the following options to define the web login page for the wireless guest users:

   Default Internal—Displays the default web login page for the controller. This is the default value.

   Customized Web Auth—Displays custom web login, login failure, and logout pages. When the customized option is selected, three separate drop-down lists for login, login failure, and logout page selection appear. You do not need to define a customized page for all three of the options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option.

   These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files. For specifics on downloading custom pages, see the "Downloading Customized Web Authentication" section on page 3-42.

   External—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

   Note External web auth is not supported for 2106 and 5500 series controllers.

   You can select specific RADIUS or LDAP servers to provide external authentication in the Security > AAA page. To do so, continue with Step 4.

Note The RADIUS and LDAP servers must be already configured to have selectable options in the Security > AAA page. You can configure these servers in the RADIUS Authentication Servers page and TACACS+ Authentication Servers page.

Step 3 If you selected External as the Web Authentication Type in Step 2, choose **Security > AAA**, and choose up to three RADIUS and LDAP servers using the drop-down lists.

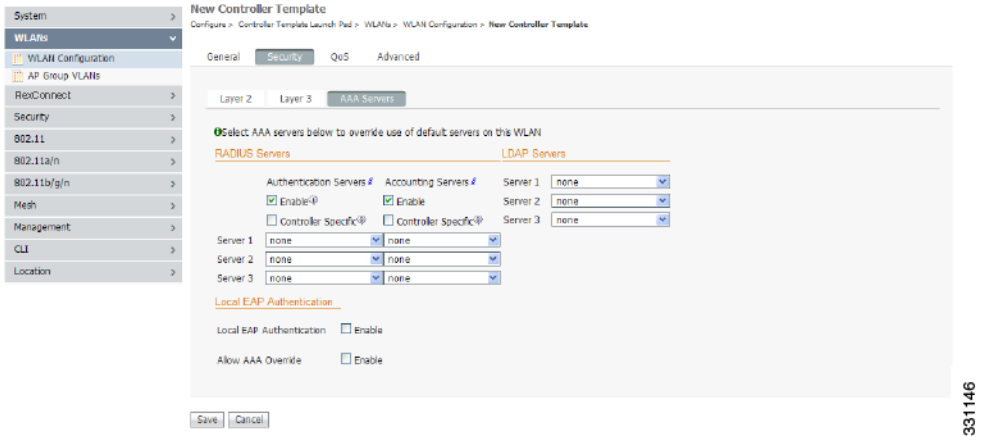
Step 4 Click **Save**.

Step 5 Repeat this process if a second (anchor) controller is being used in the network.

AAA Servers

When you click the AAA Servers tab, the AAA Servers tab appears (see Figure 10-13).

Figure 10-13 AAA Servers Tab



To configure the AAA Servers tab, follow these steps:

Step 1 Select the **Radius Server Overwrite Interface** check box to send the client authentication request through the dynamic interface which is set on the WLAN. When you enable the Radius Server Overwrite Interface option, the WLC sources all radius traffic for a WLAN using the dynamic interface configured on that WLAN.

Note You cannot enable Radius Server Overwrite Interface when Diagnostic Channel is enabled.

Note The Radius Server Overwrite Interface option is supported in controller Release 7.0.x and later.

Step 2 Select the **Enable** check boxes, then use the drop-down lists in the RADIUS and LDAP servers section to choose authentication and accounting servers. This selects the default RADIUS server for the specified WLAN and overrides the RADIUS server that is configured for the network. If all three RADIUS servers are configured for a particular WLAN, server 1 has the highest priority, and so on.

If no LDAP servers are chosen here, the NCS uses the default LDAP server order from the database.

Step 3 Select the **Interim Update** check box if you want to enable interim update for RADIUS Server Accounting. If you have selected this check box, specify the Interim Interval value. The range is 180 to 3600 seconds, and the default value is 0.

Note The Interim Interval can be entered only when Interim Update is enabled.

Step 4 Select the **Local EAP Authentication** check box if you have an EAP profile already configured that you want to enable. Local EAP is an authentication method that allows users and wireless clients to locally authenticate. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down.

Step 5 When AAA Override is enabled, and a client has conflicting AAA and controller WLAN authentication fields, client authentication is performed by the AAA server. As part of this authentication, the operating system moves clients from the default Cisco WLAN Solution to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering,

802.1X, and/or WPA operation). In all cases, the operating system also uses QoS and ACL provided by the AAA server, as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as identity networking.)

For instance, if the corporate WLAN primarily uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.

When AAA override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is only performed by the AAA server if the controller WLANs do not contain any client-specific authentication parameters.

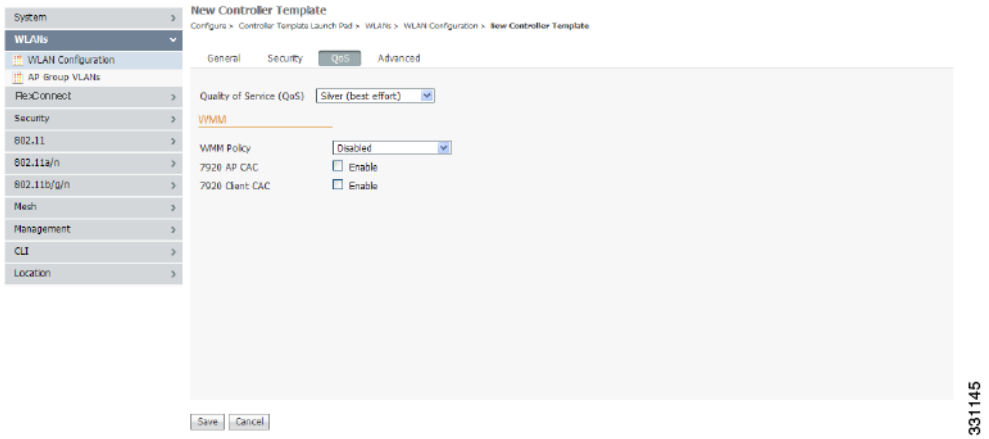
The AAA override values might come from a RADIUS server, for example.

Step 6 Click **Save**.

QoS Tab

When you click the QoS tab in the WLAN Template page, the QoS tab appears (see Figure 10-14).

Figure 10-14 QoS Tab



To configure the QoS fields, follow these steps:

Step 1 From the QoS drop-down list, choose **Platinum** (voice), **Gold** (video), **Silver** (best effort), or **Bronze** (background). Services such as VoIP should be set to gold while non-discriminating services such as text messaging can be set to bronze.

Step 2 From the WMM Policy drop-down list, choose **Disabled**, **Allowed** (so clients can communicate with the WLAN), or **Required** to make it mandatory for clients to have WMM enabled for communication.

Step 3 Select the **7920 AP CAC** check box if you want to enable support on Cisco 7920 phones.

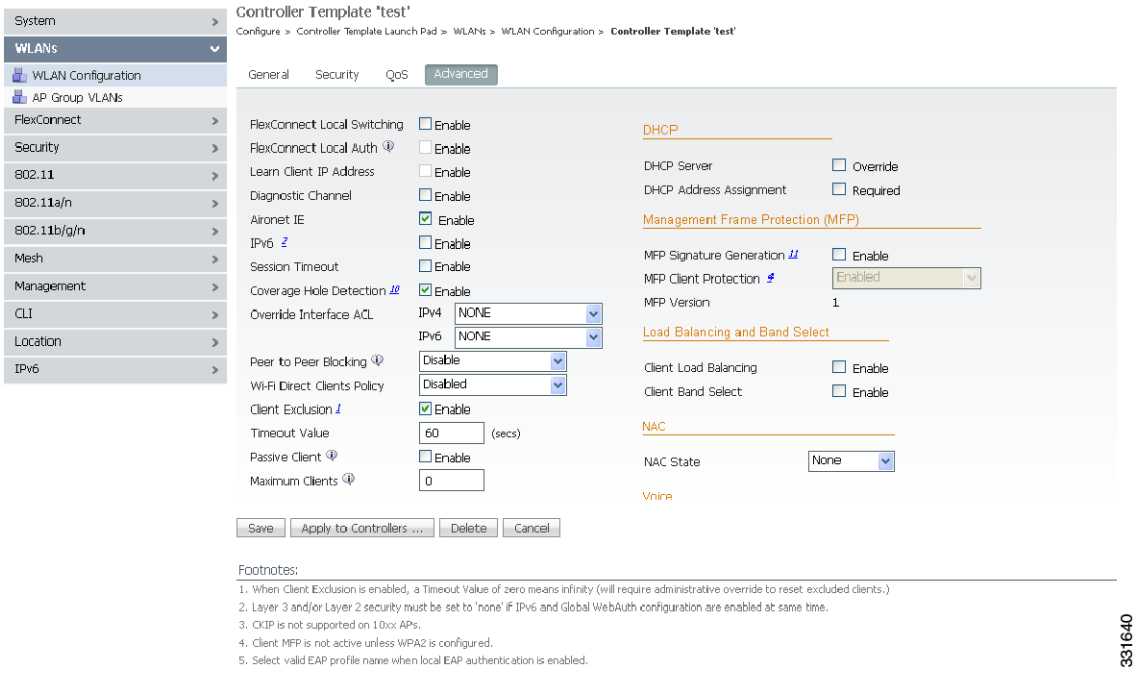
Step 4 If you want WLAN to support older versions of the software on 7920 phones, select the **7920 Client CAC** check box to enable it. The CAC limit is set on the access point for newer versions of software.

Step 5 Click **Save**.

Advanced Tab

When you click the Advanced tab in the WLAN Template page, the Advanced tab appears (see Figure 10-15).

Figure 10-15 Advanced Tab



Step 1 Select the **FlexConnect local switching** check box if you want to enable FlexConnect local switching. For more information on FlexConnect, see the "Configuring FlexConnect" section on page 12-4. If you enable it, the FlexConnect access point handles client authentication and switches client data packets locally.

FlexConnect local switching is only applicable to the Cisco 1130/1240/1250 series access points. It is not supported with L2TP or PPTP authentications, and it is not applicable to WLAN IDs 9-16.

Step 2 Select the **FlexConnect Local Auth** check box if you want to enable FlexConnect local authentication.

Local authentication is useful where you cannot maintain the criteria a remote office setup of minimum bandwidth of 128 kbps with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local switching, the authentication capabilities are present in the access point itself. Thus local authentication reduces the latency requirements of the branch office.

Note Local authentication can only be enabled on the WLAN of a FlexConnect AP that is in local switching mode.

Local authentication is not supported in the following scenarios:

- Guest Authentication cannot be performed on a FlexConnect local authentication enabled WLAN.

- RRM information is not available at the controller for the FlexConnect local authentication enabled WLAN.
- Local radius is not supported.
- Once the client has been authenticated, roaming is supported after the WLC and the other FlexConnects in the group are updated with the client information.

Step 3 When you enable hybrid-REAP local switching, the Learn Client IP Address check box is enabled by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client IP address, and the controller periodically drops the client. Disable this option so that the controller maintains the client connection without waiting to learn the client IP address. The ability to disable this option is supported only with hybrid-REAP local switching; it is not supported with hybrid-REAP central switching.

Step 4 Choose to enable the diagnostic channel feature or leave it disabled. The diagnostic channel feature allows you to troubleshoot problems regarding client communication with a WLAN. When initiated by a client having difficulties, the diagnostic channel provides the most robust communication methods with the fewest obstacles to communication.

Step 5 Select the **Aironet IE** check box if you want to enable support for Aironet information elements (IEs) for this WLAN. If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

Step 6 Select the **IPv6** check box. You can configure IPv6 bridging and IPv4 web auth on the same WLAN.

Step 7 Select the **Session Timeout** check box to set the maximum time a client session can continue before requiring reauthorization.

Step 8 Choose to enable or disable coverage hold detection (CHD) on this WLAN. By default, CHD is enabled on all WLANs on the controller. If you disable CHD on a WLAN, a coverage hole alert is still sent to the controller, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where highly mobile guests are connected to your network for short periods of time.

Step 9 The Override Interface drop-down lists provides a list of defined access control lists (ACLs). (See the "Configuring an Access Control List Template" section on page 10-73 for steps on defining ACLs.) Upon choosing an ACL from the list, the WLAN associates the ACL to the WLAN. Selecting an ACL is optional, and the default for this field is None.

Step 10 You can configure peer-to-peer blocking per WLAN rather than applying the status to all WLANs. From the Peer to Peer Blocking drop-down list, choose one of the following:

- Disable—Peer-to-peer blocking is disabled, and traffic is bridged locally whenever possible.
- Drop—The packet is discarded.
- Forward Up Stream—The packet is forwarded on the upstream VLAN, and the decision is made about what to do with the packet.

Note For controller Release 7.2.x and later, the Forward Up Stream is same as Drop for locally switched clients.

If FlexConnect local switching is enabled for the WLAN, which prevents traffic from passing through the controller, this drop-down list is dimmed.

Note Peer-to-peer blocking does not apply to multicast traffic.

Step 11 From the Wi-Fi Direct Clients Policy drop-down list, choose one of the following options:

- **Disabled**—Disables the Wi-Fi Direct Clients Policy for the WLAN and deauthenticates all Wi-Fi Direct capable clients. The default is Disabled.
- **Allow**—Allows the Wi-Fi Direct clients to associate with an infrastructure WLAN.
- **Not-Allow**—Disallows the Wi-Fi Direct clients from associating with an infrastructure WLAN.

Note The Wi-Fi Direct Clients Policy is applicable to WLANs that have APs in local mode only.

Note The Wi-Fi Direct Clients Policy is applicable for controller Release 7.2.x. and later.

Step 12 Select the check box if you want to enable automatic client exclusion.

Step 13 If you enable client exclusion, you must also set the Timeout Value in seconds for disabled client machines. Client machines are excluded by MAC address, and their status can be observed. A timeout setting of 0 indicates that administrative control is required to reenable the client.

Note When session timeout is not set, it implies that an excluded client remains and does not timeout from the excluded state. It does not imply that the exclusion feature is disabled.

Step 14 Enter the maximum number of clients to be associated in a WLAN in the Maximum Clients text box. The valid range is from 0 to 7000. The default value is 0.

Note A value of 0 allows unlimited number of clients to be associated with a WLAN.

Step 15 Enable dynamic anchoring of static IP clients by selecting the **Static IP Tunneling** check box.

Step 16 Select the **Media Session Snooping** check box. This feature enables access points to detect the establishment, termination, and failure of voice calls and then report them to the controller and the NCS. It can be enabled or disabled per WLAN.

When media session snooping is enabled, the access point radios that advertise this WLAN snoop for Session Initiation Protocol (SIP) voice packets. Any packets destined to or originating from port number 5060 are considered for further inspection. The access point tracks whether Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, already on an active call, or in the process of ending a call and then notify the controller of any major call events.

Step 17 Select the **KTS based CAC** check box to enable KTS based CAC support per WLAN.

WLC supports TSPEC based CAC and SIP based CAC. But there are certain phones that work with different protocols for CAC, which are based on the KTS (Key Telephone System). For supporting CAC with KTS-based SIP clients, WLC should understand and process the bandwidth request message from those clients to allocate the required bandwidth on the AP radio, in addition to handling and sending certain other messages, as part of this protocol.

Note The KTS CAC configuration is only supported by Cisco 5508, 7500, WISM2, and 2500 controllers that run controller software Release 7.2.x. This feature is not supported by Cisco 4400 series controllers.

Step 18 NAC State—From the **NAC State** drop-down list, choose **SNMP NAC** or **Radius NAC**. SIP errors that are discovered generate traps that appear on the client troubleshooting and alarms screens. The controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing. See the "NAC Integration" section on page 8-44 for more information.

Step 19 Off-Channel Scanning Defer is essential to the operation of RRM, which gathers information about alternate channel choices such as noise and interference. Additionally, Off-Channel Scanning Defer is responsible for rogue detection. Devices that need to defer Off-Channel Scanning Defer should use the same WLAN as often as possible. If there are many of these devices (and the possibility exists that Off-Channel Defer scanning could be completely disabled by the use of this feature), you should implement an alternative to local AP Off-Channel Scanning Defer, such as monitor access points, or other access points in the same location that do not have this WLAN assigned.

Assignment of a QoS policy (bronze, silver, gold, and platinum) to a WLAN affects how packets are marked on the downlink connection from the access point regardless of how they were received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. The marking results of each QoS policy are as follows:

- Bronze marks all downlink traffic to UP= 1.
- Silver marks all downlink traffic to UP= 0.
- Gold marks all downlink traffic to UP=4.
- Platinum marks all downlink traffic to UP=6.

Set the Scan Defer Priority by clicking the priority argument and Set the time in milliseconds in the Scan Defer Interval text box. Valid values are 0 through 60000. The default value is 100 milliseconds.

Step 20 In 802.11a/n and 802.11b/g/n networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Normally, the DTIM value is set to 1 (transmit broadcast and multicast frames after every beacon) or 2 (transmit after every other beacon). For instance, if the beacon period of the 802.11a/n or 802.11b/g/n network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames 10 times per second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames 5 times per second. Either of these settings might be suitable for applications, including VoIP, that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (transmit broadcast and multicast frames after every 255th beacon) if all 802.11a/n or 802.11b/g/n clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently, resulting in longer battery life. For instance, if the beacon period is 100 ms and the DTIM value is set to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds, allowing the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, resulting in longer battery life.

Many applications cannot tolerate a long time between broadcast and multicast messages, resulting in poor protocol and application performance. We recommend a low DTIM value for 802.11a/n and 802.11b/g/n networks that support such clients.

Under DTIM Period, enter a value between 1 and 255 (inclusive) in the 802.11a/n and 802.11b/g/n fields. The default value is 1 (transmit broadcast and multicast frames after every beacon).

Step 21 When you select the check box to override DHCP server, another field appears where you can enter the IP address of your DHCP server. For some WLAN configurations, this is required. Three valid configurations are as follows:

- DHCP Required and a valid DHCP server IP address - All WLAN clients obtain an IP address from the DHCP server.
- DHCP is not required and a valid DHCP server IP address - All WLAN clients obtain an IP address from the DHCP server or use a static IP address.
- DHCP not required and DHCP server IP address 0.0.0.0 - All WLAN clients are forced to use a static IP address. All DHCP requests are dropped.

You cannot choose to require a DHCP address assignment and then enter a DHCP server IP address.

Step 22 If the MFP Signature Generation check box is selected, it enables signature generation for the 802.11 management frames transmitted by an access point associated with this WLAN. Signature generation makes sure that changes to the transmitted management frames by an intruder are detected and reported.

Step 23 From the MFP Client Protection drop-down list, choose **Enabled**, **Disabled**, or **Required** for configuration of individual WLANs of a controller. If infrastructure MFP is not enabled, this drop-down list is unavailable.

Note The Enabled parameter is the same as the Optional parameter that you choose from the MFP Client Protection drop-down list in the WLC graphical user interface.

Note Client-side MFP is only available for those WLANs configured to support Cisco Compatible Extensions (version 5 or later) clients, and WPA2 must first be configured.

Step 24 Enter a value between 1 and 255 beacon intervals in the 802.11a/n DTIM Period group box of the page. The controller sends a DTIM packet on the 802.11a/n radio for this WLAN based on what is entered as an interval.

Step 25 Enter a value between 1 and 255 beacon intervals in the 802.11b/g/n DTIM Period group box of the page. The controller sends a DTIM packet on the 802.11b/g/n radio for this WLAN based on what is entered as an interval.

Note The DTIM configuration is not appropriate for guest LANs.

Step 26 Select the **Client Profiling** check box to enable or disable profiling of all the clients that are associated with the WLAN.

Note Client Profiling is not supported with FlexConnect local authentication.

Note Client Profiling is configurable only when you select the DHCP Address Assignment check box.

Step 27 Click **Save**.

Configuring WLAN AP Groups Templates

Site-specific VLANs or AP groups limit the broadcast domains to a minimum by segmenting a WLAN into different broadcast domains. Benefits include more effective management of load balancing and bandwidth allocation.

To configure WLAN AP Groups, follow these steps:

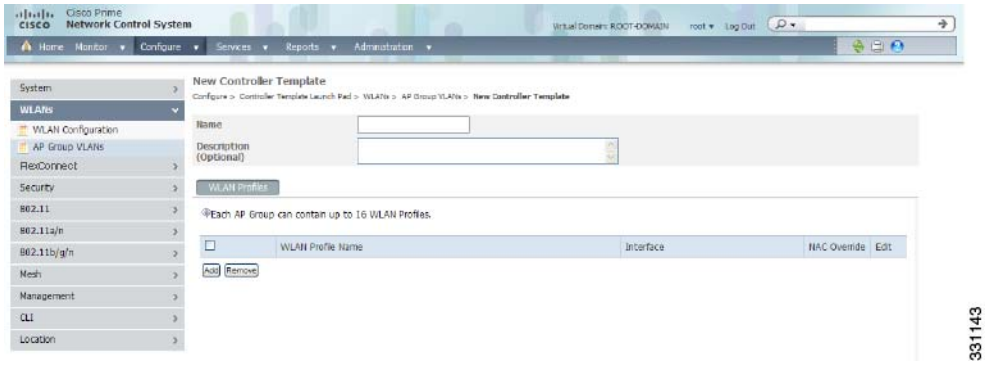
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **AP Groups** or choose **WLAN > AP Groups** from the left sidebar menu. The WLAN > AP Groups page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The AP Groups template page appears (see Figure 10-16).

Figure 10-16 WLAN AP Groups



This page displays a summary of the AP groups configured on your network. In this page, you can add, remove, edit, or view details of an AP group. Click in the Edit column to edit its access point(s). Select the check box in the WLAN Profile Name column, and click **Remove** to delete WLAN profiles.

Note The maximum characters that you can enter in the Description text box is 256.

Adding Access Point Groups

You can create or modify a template for dividing the WLAN profiles into AP groups.

To add a new access point group, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **AP Group VLANs** or choose **WLAN > AP Group VLANs** from the left sidebar menu.

Note AP Groups (for controllers Release 5.2 and later) are referred to as AP Group VLANs for controllers prior to 5.2.

Step 3 Choose **Add Template** from the Select a command drop-down list, and click **Go**.

Step 4 Enter a name and group description for the access point group.

Note The group description is optional.

Step 5 If you want to add a WLAN profile, click the **WLAN Profiles** tab and configure the following fields:

a. Click **Add**.

Note To display all available WLAN profile names, delete the current WLAN profile name from the text box. When the current WLAN profile name is deleted from the text box, all available WLAN profiles appear in the drop-down list.

Note Each access point is limited to 16 WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.

Note The WLAN override feature applies only to older controllers that do not support the 512 WLAN feature (can support up to 512 WLAN profiles).

b. Type a WLAN profile name or choose one from the WLAN Profile Name drop-down list.

c. Enter an interface/interface group or choose one from the Interface/Interface Group drop-down list.

Note To display all available interfaces, delete the current interface from the Interface text box. When the current interface is deleted from the Interface text box, all available interfaces appear in the drop-down list.

d. Select the **NAC Override** check box, if applicable. The NAC override feature is disabled by default.

e. When access points and WLAN profiles are added, click **Save**.

Step 6 If you want to add a RF profile, click the **RF Profiles** tab, and configure the following fields:

- 802.11a—Drop-down list from which you can choose an RF profile for APs with 802.11a radios.
- 802.11b—Drop-down list from which you can choose an RF profile for APs with 802.11b radios.
- When RF profiles are added, click **Save**.

Note Click the **Click here** link to add a new RF profile. See the "Configuring RF Profiles Templates (802.11)" section on page 10-92 for more information.

Deleting Access Point Groups

To delete an access point group, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **AP Groups** or choose **WLAN > AP Groups** from the left sidebar menu.

Step 3 Click **Remove**.

Configuring FlexConnect Templates

This section contains the following topics:

Configuring FlexConnect AP Groups Templates

FlexConnect enables you to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. There is no deployment restriction on the number of FlexConnect access points per location, but you can organize and group the access points per floor and limit them to 25 or so per building, because it is likely the branch offices share the same configuration.

To set up an FlexConnect AP group, follow these steps:

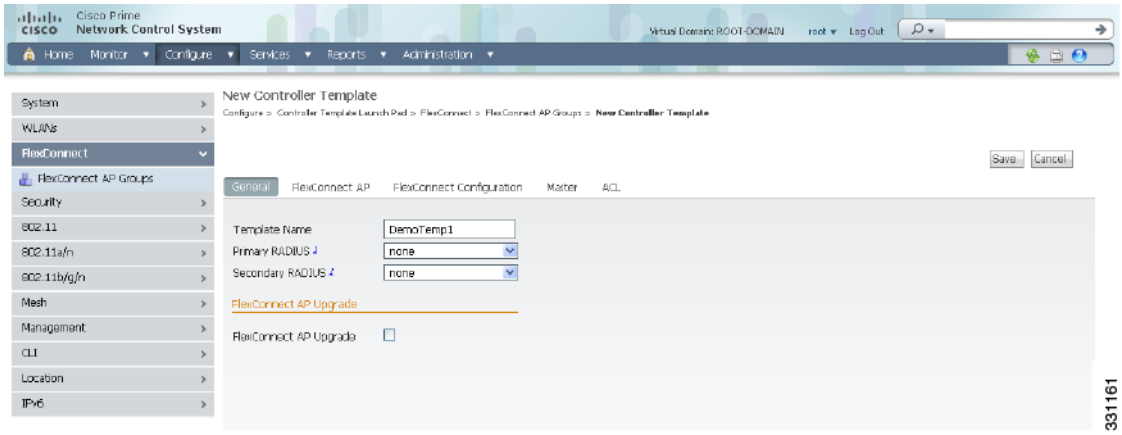
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **FlexConnect AP Groups** or choose **FlexConnect > FlexConnect AP Groups** from the left sidebar menu. The FlexConnect > FlexConnect AP Groups page appears. It displays the primary and secondary RADIUS, as well as the number of controllers and virtual domains that the template is applied to, which automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The General tab of the FlexConnect AP Groups page appears (see Figure 10-17).

Figure 10-17 AP Groups FlexConnect Template



Step 4 The Template Name field shows the group name assigned to the FlexConnect access point group.

Step 5 Choose the primary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, the NCS configured RADIUS server does not apply. A value of 10 indicates that the primary RADIUS server is not configured for this group.

Step 6 Choose the secondary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, the NCS configured RADIUS server does not apply. A value of 0 indicates that the primary RADIUS server is not configured for this group.

Step 7 If you want to add an access point to the group, click the **FlexConnect AP** tab.

Step 8 An access point Ethernet MAC address cannot exist in more than one FlexConnect group on the same controller. If more than one group is applied to the same controller, select the **Ethernet MAC** check box to unselect an access point from one of the groups. You should save this change or apply it to controllers.

Step 9 Click **Add AP**. The FlexConnect AP Group page appears.

Step 10 Click the **FlexConnect Configuration** tab to enable local authentication for a FlexConnect group.

Note Make sure that the Primary RADIUS Server and Secondary RADIUS Server fields are set to **None** on the General tab.

Step 11 Select the **FlexConnect Local Authentication** check box to enable local authentication for this FlexConnect group. The default value is unselected.

Note When you attempt to use this feature, a warning message indicates that it is a licensed feature.

Note You can click the **Users configured in the group** link that appears at the bottom of the page to view the list of FlexConnect users. You can create FlexConnect users only after you save the FlexConnect AP Group.

Step 12 To allow a FlexConnect access point to authenticate clients using LEAP, select the **LEAP** check box. Otherwise, to allow a FlexConnect access point to authenticate clients using EAP-FAST, select the **EAP-FAST** check box.

Step 13 Perform one of the following, depending on how you want Protected Access Credentials (PACs) to be provisioned:

- To use manual PAC provisioning, enter the key used to encrypt and decrypt PACs in the EAP-FAST Key and Confirm EAP-FAST Key text boxes. The key must be 32 hexadecimal characters.
- To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select the **Auto key generation** check box.

Step 14 In the EAP-FAST Key text box, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.

Step 15 In the EAP-FAST Authority ID text box, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.

Step 16 In the EAP-FAST Authority Info text box, enter the authority information of the EAP-FAST server.

Step 17 In the EAP-FAST Pac Timeout text box, specify a PAC timeout value by entering the number of seconds for the PAC to remain viable in the edit box. The valid range is 2 to 4095 seconds.

Note The EAP-FAST options are available only if you select the **EAP-FAST** check box in Step 12.

Step 18 Click the **Image Upgrade** tab and configure the following:

- FlexConnect AP Upgrade—Select the check box if you want to upgrade the FlexConnect access points.
- Slave Maximum Retry Count—Enter the maximum retries for the slave to undertake to start the download from the master in the FlexConnect group. This option is available only if you select the FlexConnect AP Upgrade check box.

Note You are allowed to add an access point as a master access point only if the FlexConnect AP Upgrade check box is enabled on the General tab.

Step 19 Click the **VLAN-ACL Mapping** tab to view, add, edit, or remove a VLAN ACL mapping.

a. Click **Add**.
b. Enter a VLAN ID. The valid VLAN ID range is 1—4094.
c. From the Ingress ACL drop-down list, choose an Ingress ACL.
d. From the Egress AC drop-down list, choose an Egress ACL.
e. Click **Save**.

Step 20 Click the **WLAN-ACL Mapping** tab to view, add, edit, or remove a WLAN ACL mapping.

a. Click **Add**.
b. From the WLAN Profile Name drop-down list, choose a WLAN profile.

c. From the WebAuth ACL drop-down list, choose a WebAuth ACL.

d. Click **Save**.

Note You can add up to a maximum of 16 WebAuth ACLs.

Step 21 Click the **WebPolicy ACL** tab to view, add, edit, or remove a WebPolicy ACL mapping.

a. Click **Add**.

b. From the Web-Policy ACL drop-down list, choose a WebPolicy ACL.

c. Click **Save**.

Note You can add up to a maximum of 16 Web-Policy ACLs.

Step 22 Click **Save**.

Configuring FlexConnect Users

Note You can create FlexConnect users only after you save the FlexConnect AP Group.

Note Maximum 100 FlexConnect users are supported in controller Release 5.2.x.x and later. If controller Release 5.2.0.0, and earlier supports only 20 FlexConnect users.

To configure a FlexConnect user, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **FlexConnect AP Groups** or choose **FlexConnect > FlexConnect AP Groups** from the left sidebar menu. The FlexConnect > FlexConnect AP Groups page appears.

Step 3 Click the **FlexConnect Configuration** tab to enable local authentication for a FlexConnect group.

Step 4 Select the **FlexConnect Local Authentication** check box to enable local authentication for this FlexConnect group.

Step 5 Click the **Users configured in the group** link. The FlexConnect Users page appears.

Step 6 If you want to add a new user, choose **Add User** from the Select a command drop-down list, and click **Go**. The **Add User** page appears.

Step 7 In the User Name text box, enter the FlexConnect username.

Step 8 In the Password text box, enter the password.

Step 9 Reenter the password in the Confirm Password text box.

Step 10 Click **Save**.

Note To delete a FlexConnect User, choose a user from the FlexConnect Users list, and then click **Delete**.

Configuring Security Templates

This section contains the following topics:

Configuring a General Security Controller Template

To add a new template with general security information for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **New** beside the template you want to add.

Step 3 Configure the following fields:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Maximum Local Database Entries (on next reboot)—Enter the maximum number of allowed database entries. This amount becomes effective on the next reboot.

Step 4 Click **Save**. Once saved, the template appears in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 10-2 for more information.

Configuring a File Encryption Template

This page enables you to add a file encryption template or make modifications to an existing file encryption template.

To configure a File Encryption template, follow these steps:

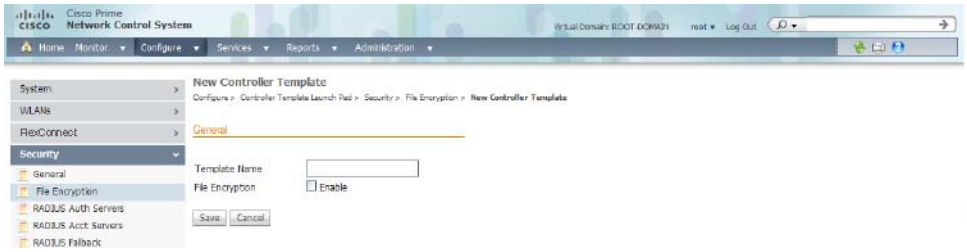
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **File Encryption** or choose **Security > File Encryption** from the left sidebar menu. The Security > File Encryption page appears. The number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The File Encryption template page appears (see Figure 10-18).

Figure 10-18 File Encryption Template



Step 4 Check if you want to enable file encryption.

Step 5 Enter an encryption key text string of exactly 16 ASCII characters.

Step 6 Retype the encryption key.

Step 7 Click **Save**.

Configuring a RADIUS Authentication Template

This page allows you to add a RADIUS authentication template or make modifications to an existing template. After these server templates are configured, controller users who log into the controller through the CLI or GUI are authenticated.

To configure a RADIUS Authentication template, follow these steps:

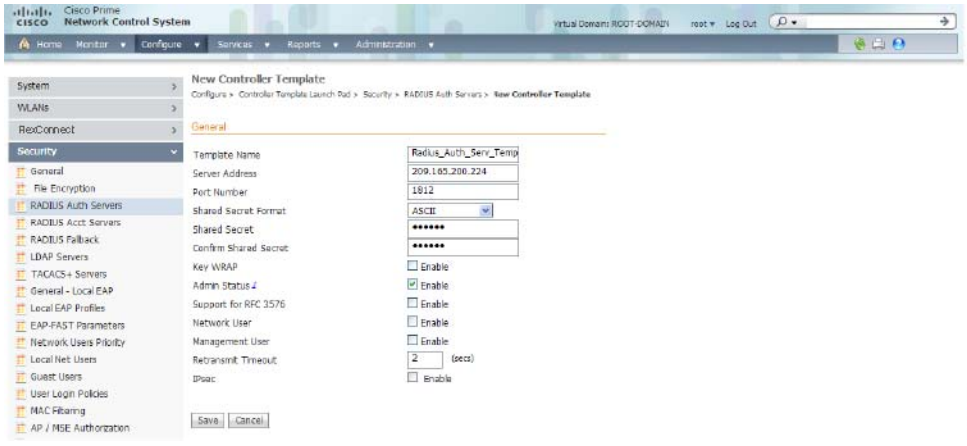
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **RADIUS Auth Servers** or choose **Security > RADIUS Auth Servers** from the left sidebar menu. The Security > RADIUS Auth Servers page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The IP address of the RADIUS server and the port number and admin status for the interface protocol is also displayed. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The RADIUS Auth Servers template page appears (see Figure 10-19).

Figure 10-19 RADIUS Authentication Server Template



Step 4 From the Shared Secret Format drop-down list, choose either **ASCII** or **hex**.

Note Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and the NCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.

Step 5 Enter the RADIUS shared secret used by your specified server.

Step 6 Select the check box if you want to enable key wrap. If this check box is enabled, the authentication request is sent to RADIUS servers that have following key encryption key (KEK) and message authenticator code keys (MACK) configured. When enabled, the following fields appear:

- Shared Secret Format: Enter ASCII or hexadecimal.

Note Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and the NCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in the event a discovered template is applied to another device.

- KEK Shared Secret: Enter the KEK shared secret.
- MACK Shared Secret: Enter the MACK shared secret.

Note Each time the controller is notified with the shared secret, the existing shared secret is overwritten with the new shared secret.

Step 7 Click if you want to enable administration privileges.

Step 8 Click if you want to enable support for RFC 3576. RFC 3576 is an extension to the Remote Authentication Dial In User Service (RADIUS) protocol. It allows dynamic changes to a user session and includes support for disconnecting users and changing authorizations applicable to a user session. With these authorizations, support is provided for Disconnect and Change-of-Authorization (CoA) messages. Disconnect messages immediately terminate a user session, whereas CoA messages modify session authorization attributes such as data filters.

Step 9 Click if you want to enable network user authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.

Step 10 Click if you want to enable management authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the management user.

Step 11 Specify the time in seconds after which the RADIUS authentication request times out and a retransmission is attempted by the controller. You can specify a value between 2 and 30 seconds.

Step 12 If you click to enable the IP security mechanism, additional IP security fields are added to the page, and Steps 13 to 19 are required. If you disable it, click **Save** and skip Steps 13 to 19.

Step 13 Use the drop-down list to choose which IP security authentication protocol to use. The options are **HMAC-SHA1**, **HMAC-MD5**, and **None**.

Message Authentication Codes (MAC) are used between two parties that share a secret key to validate information transmitted between them. HMAC (Hash MAC) is a mechanism based on cryptographic hash functions and can be used in combination with any iterated cryptographic hash function. HMAC-MD5 and HMAC-SHA1 are two constructs of the HMAC using the MD5 hash function and the SHA1 hash function. HMAC also uses a secret key for calculation and verification of the message authentication values.

Step 14 Set the IP security encryption mechanism to use. The options are as follows:

- DES—Data Encryption Standard is a method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.
- Triple DES—Data Encryption Standard that applies three keys in succession.
- AES 128 CBC—Advanced Encryption Standard uses keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits. AES 128 CBC uses a 128-bit data path in Cipher Clock Chaining (CBC) mode.
- None—No IP security encryption mechanism.

Step 15 The Internet Key Exchange (IKE) authentication is not an editable text box. Internet Key Exchange protocol (IKE) is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how data should be protected. IKE keeps track of connections by assigning a bundle of security associations (SAs) to each connection.

Step 16 Use the IKE phase 1 drop-down list to choose either aggressive or main. This sets the IKE protocol. IKE phase 1 is used to negotiate how IKE is protected. Aggressive mode passes more information in fewer packets, with the benefit of a slightly faster connection, at the cost of transmitting the identities of the security gateways in the clear.

Step 17 At the Lifetime field, set the timeout interval (in seconds) when the session expires.

Step 18 Set the IKE Diffie Hellman group. The options are group 1 (768 bits), group 2 (1024 bits), or group 5 (1536 bits). Diffie-Hellman techniques are used by two devices to generate a symmetric key where you can publicly exchange values and generate the same symmetric key.

Although all three groups provide security from conventional attacks, Group 5 is considered more secure because of its larger key size. However, computations involving Group 1 and Group 2 based keys might occur slightly faster because of their smaller prime number size.

Step 19 Click **Save**.

Configuring a RADIUS Accounting Template

This page allows you to add a RADIUS accounting template or make modifications to an existing RADIUS accounting template.

To configure a RADIUS Accounting template, follow these steps:

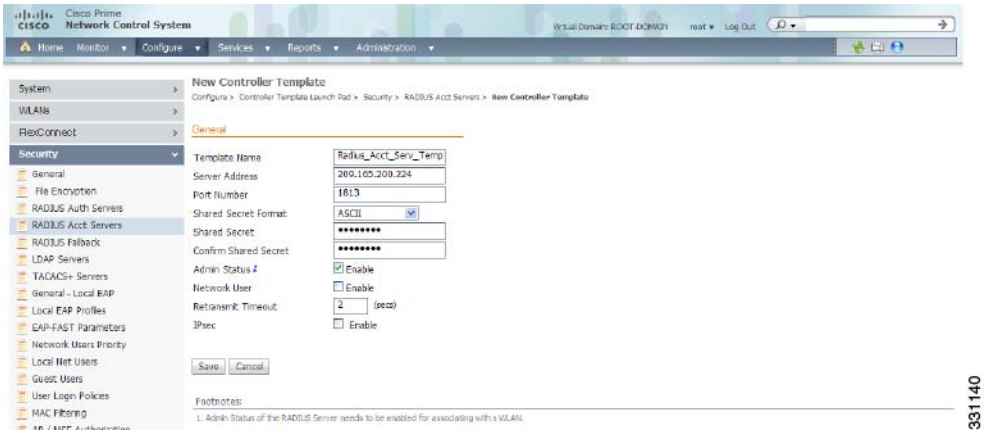
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **RADIUS Acct Servers** or choose **Security > RADIUS Acct Servers** from the left sidebar menu. The Security > RADIUS Acct Servers page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The IP address of the RADIUS server and the port number and admin status for the interface protocols are also displayed. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The RADIUS Accounting Server template page appears (see Figure 10-20).

Figure 10-20 RADIUS Accounting Server Templates



Step 4 Use the Shared Secret Format drop-down list to choose either **ASCII** or **hexadecimal**.

Note Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and the NCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.

Step 5 Enter the RADIUS shared secret used by your specified server.

Step 6 Retype the shared secret.

Step 7 Click if you want to establish administrative privileges for the server.

Step 8 Click if you want to enable the network user authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.

Step 9 Specify the time in seconds after which the RADIUS authentication request times out and a retransmission by the controller occurs. You can specify a value between 2 and 30 seconds.

Step 10 Click **Save**.

Configuring a RADIUS Fallback Template

This page allows you to add a RADIUS fallback template or make modifications to an existing RADIUS fallback template.

To configuring a RADIUS Fallback template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **RADIUS Fallback** or choose **Security > RADIUS Fallback** from the left sidebar menu. The Security > RADIUS Fallback page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The RADIUS Fallback template page appears (see Figure 10-21).

Figure 10-21 RADIUS Fallback Page

Step 4 From the RADIUS Fallback Mode drop-down list, choose **Off**, **Passive**, or **Active**.

- Off—Disables fallback.
- Passive—You must enter a time interval.
- Active—You must enter a username and time interval.

Step 5 Click **Save**.

Configuring an LDAP Server Template

This section explains how to configure a Lightweight Directory Access Protocol (LDAP) server as a backend database, similar to a RADIUS or local user database. An LDAP backend database allows the controller to query an LDAP server for the credentials (username and password) of a particular user. These credentials are then used to authenticate the user. For example, local EAP might use an LDAP server as its backend database to retrieve user credentials.

To add an LDAP server template or make modifications to an existing LDAP server template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **LDAP Servers** or choose **Security > LDAP Servers** from the left sidebar menu. The Security > LDAP Servers page appear. The IP address of the LDAP server and the port number for the interface protocols are displayed. Also, the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The LDAP Server template page appears (see Figure 10-22).

Figure 10-22 LDAP Server Template

Step 4 The port number of the controller to which the access point is connected.

Step 5 From the Bind Type drop-down list, choose **Authenticated** or **Anonymous**. If you choose Authenticated, you must enter a bind username and password as well. A bind is a socket opening that performs a lookup. Anonymous bind requests are rejected.

Step 6 In the Server User Base DN text box, enter the distinguished name of the subtree in the LDAP server that contains a list of all the users.

Step 7 In the Server User Attribute text box, enter the attribute that contains the username in the LDAP server.

Step 8 In the Server User Type text box, enter the ObjectType attribute that identifies the user.

Step 9 In the Retransmit Timeout text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

Step 10 Select the **Admin Status** check box if you want the LDAP server to have administrative privileges.

Step 11 Click **Save**.

Configuring a TACACS+ Server Template

This page allows you to add a TACACS+ server or make modifications to an existing TACACS+ server template. After these server templates are configured, controller users who log into the controller through the CLI or GUI are authenticated.

To configure a TACACS+ Server template, follow these steps:

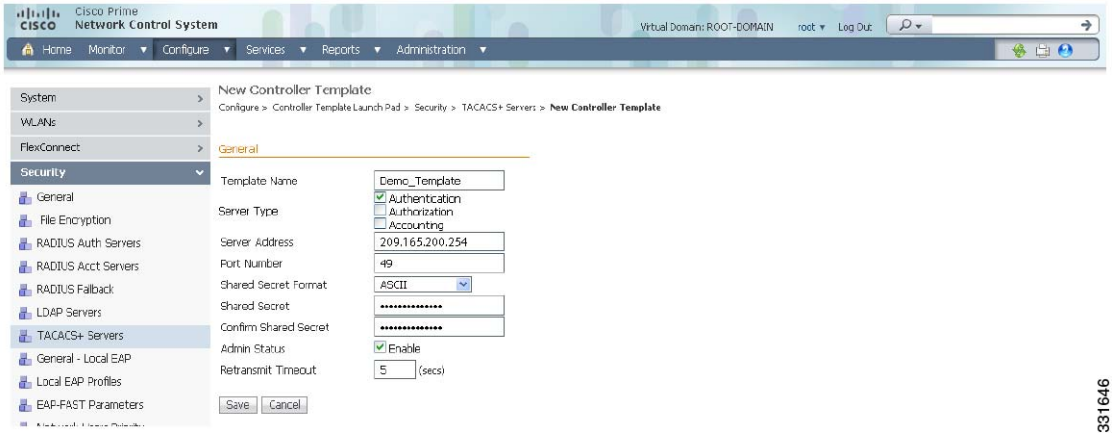
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **TACACS+ Server** or choose **Security > TACACS+ Server** from the left sidebar menu. The Security > TACACS+ Servers page appears. The IP address and the port number and admin of the TACACS+ template are displayed. Also, the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The TACACS+ Servers template page appears (see Figure 10-23).

Figure 10-23 TACACS+ Server Template



Step 4 Select one or more server types by selecting their respective check boxes. The following server types are available:

- **authentication**—Server for user authentication/authorization.
- **authorization**—Server for user authorization only.
- **accounting**—Server for RADIUS user accounting.

Step 5 Enter the IP address of the server.

Step 6 Enter the port number of the server. The default is 49.

Step 7 From the drop-down list, choose either **ASCII** or **hex**.

Note Regardless of which format you choose, for security reasons, only ASCII is visible on the WLC (and the NCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. Set the key format again in the template in the event a discovered template is applied to another device.

Step 8 Enter the TACACS+ shared secret used by your specified server in the Shared Secret text box.

Step 9 Reenter the shared secret in the Confirm Shared Secret text box.

Step 10 Select the **Admin Status** check box if you want the TACACS+ server to have administrative privileges.

Step 11 In the Retransmit Timeout text box, enter the time, in seconds, after which the TACACS+ authentication request times out and a retransmission is attempted by the controller.

Step 12 Click **Save**.

Configuring a Local EAP General Template

This page allows you to specify a timeout value for local EAP. You can then add or make changes to an existing local EAP general template.

Note If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Local EAP General** or choose **Security > Local EAP General** from the left sidebar menu. The Security > Local EAP General page appears. The number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Local EAP General controller template page appears (see Figure 10-24).

Figure 10-24 Local EAP General Template

Step 4 In the Local Auth Active Timeout text box, enter the amount of time (in seconds) that the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fail. The valid range is 1 to 3600 seconds, and the default setting is 1000 seconds.

Step 5 The following values should be adjusted if you are using EAP-FAST, manual password entry, one-time password, or 7920/7921 phones. You must increase the 802.1x timeout values on the controller (default=2 seconds) for the client to obtain the PAC using automatic provisioning. The recommended and default timeout on the Cisco ACS server is 20 seconds.

Note Roaming fails if these values are not set the same across multiple controllers.

- Local EAP Identify Request Timeout =1
- Local EAP Identity Request Maximum Retries=20
- Local EAP Dynamic WEP Key Index=0
- Local EAP Request Timeout=20
- Local EAP Request Maximum Retries=2

Step 6 Click **Save**.

Configuring a Local EAP Profile Template

This page allows you to add a local EAP profile template or make modifications to an existing template. Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, thereby removing dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users.

Note The LDAP backend database supports only these local EAP methods: EAP-TLS and EAP-FAST with certificates. LEAP and EAP-FAST with PACs are not supported for use with the LDAP backend database.

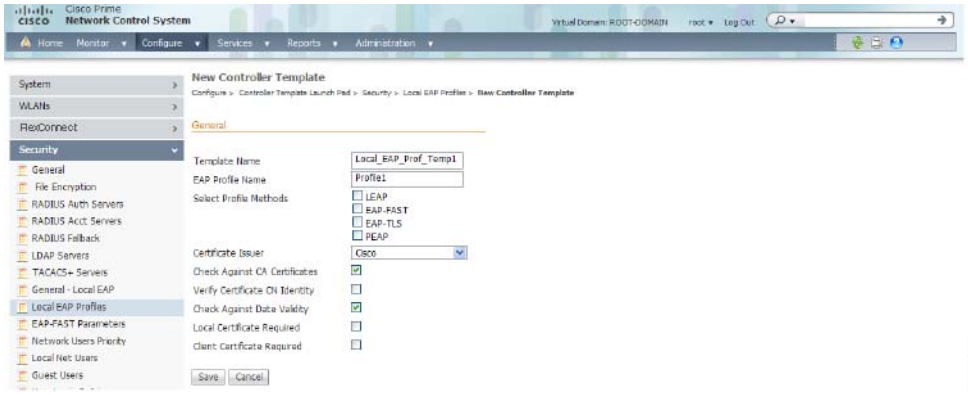
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Local EAP Profiles** or choose **Security > Local EAP Profiles** from the left sidebar menu. The Security > Local EAP Profiles page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. It also shows the EAP profile name and indicates whether LEAP, EAP-FAST, TLS, or PEAP is used. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Local EAP Profiles template page appears (see Figure 10-25).

Figure 10-25 Local EAP Profiles Template



Step 4 Each EAP profile must be associated with an authentication type(s). Choose the desired authentication type:

- LEAP—This authentication type leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. A username and password are used to perform mutual authentication with the RADIUS server through the access point.
- EAP-FAST—This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1X EAP mutual authentication. A username, password, and PAC (protected access credential) are used to perform mutual authentication with the RADIUS server through the access point.
- TLS—This authentication type uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It requires a client certificate for authentication.
- PEAP—This authentication type is based on EAP-TLS authentication but uses a password instead of a client certificate for authentication. PEAP uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.

Step 5 Use the Certificate Issuer drop-down list to determine whether Cisco or another vendor issued the certificate for authentication. Only EAP-FAST and TLS require a certificate.

Step 6 If you want the incoming certificate from the client to be validated against the certificate authority (CA) certificates on the controller, select the **Check Against CA Certificates** check box.

Step 7 If you want the (CN) in the incoming certificate to be validated against the common name of the CA certificate, select the **Verify Certificate CN Identity** check box.

Step 8 If you want the controller to verify that the incoming device certificate is still valid and has not expired, select the **Check Against Date Validity** check box.

Step 9 If a local certificate is required, select the check box.

Step 10 If a client certificate is required, select the check box.

Step 11 Click **Save**.

Step 12 To enable local EAP, follow these steps:

a. Choose **WLAN > WLAN Configuration** from the left sidebar menu.

b. Click the profile name of the desired WLAN.

c. Choose the **Security > AAA Servers** tab to access the AAA Servers page.

d. Select the **Local EAP Authentication** check box to enable local EAP for this WLAN.

Step 13 Click **Save**.

Configuring an EAP-FAST Template

This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1X EAP mutual authentication. A username, password, and PAC are used to perform mutual authentication with the RADIUS server through the access point. This page allows you to add an EAP-FAST template or make modifications to an existing EAP-FAST template.

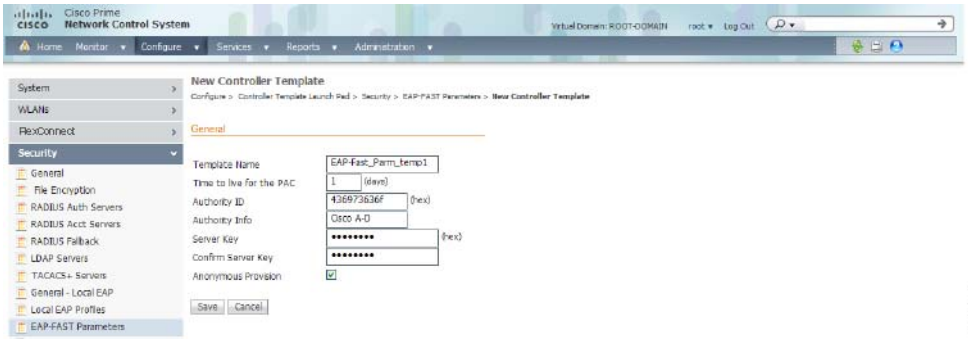
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **EAP-FAST Parameters** or choose **Security > EAP-FAST Parameters** from the left sidebar menu. The Security > EAP-FAST Parameters page appears. The number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The EAP-FAST Parameters template page appears (see Figure 10-26).

Figure 10-26 EAP-FAST Parameters Template



Step 4 In the Time to Live for the PAC text box, enter the number of days for the PAC to remain viable. The valid range is 1 to 1000 days, and the default setting is 10 days.

Step 5 In the Authority ID text box, enter the authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters, but you must enter an even number of characters.

Step 6 In the Authority Info text box, enter the authority identifier of the local EAP-FAST server in text format.

Step 7 In the Server Key and Confirm Server Key text boxes, enter the key (in hexadecimal characters) used to encrypt and decrypt PACs.

Step 8 If you want to enable anonymous provisioning, select the **Anonymous Provision** check box. This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If you disable this feature, PACs must be manually provisioned.

Step 9 Click **Save**.

Configuring a Network User Priority Template

You can specify the order that LDAP and local databases use to retrieve user credential information. This page allows you to add or make modifications to an existing network user credential retrieval priority template.

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Network Users Priority** or choose **Security > Network Users Priority** from the left sidebar menu. The Security > Network User Credential Retrieval Priority page appears. The network retrieval order and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Network Users Priority template page appears (see Figure 10-27).

Figure 10-27 Network User Credential Retrieval Priority Order Template

Step 4 Use the left and right pointing arrows to include or exclude network user credentials in the right page.

Step 5 Use the up and down buttons to determine the order credentials are tried.

Step 6 Click **Save**.

Configuring a Local Network Users Template

With this template, you can store the credentials (username and password) of all the local network users. These credentials are then used to authenticate the users. For example, local EAP might use the local user database as its backend database to retrieve user credentials. This page allows you to add or make modifications to an existing local network user template. You must create a local net user and define a password when logging in as a web authentication client.

To configure a Local Network Users template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Local Net Users** or choose **Security > Local Net Users** from the left sidebar menu. The Security > Local Net Users page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Local Net Users template page appears (see Figure 10-28).

Figure 10-28 Local Net Users Template

Step 4 If you keep Import from File enabled, you need to enter a file path or click **Browse** to navigate to the file path. Then continue to Step 11. If you disable the import, continue to Step 5.

Note You can only import a .csv file. Any other file formats are not supported.

The first row in the file is the header. The data in the header is not read by the NCS. The header can either be blank or filled. The NCS reads data from the second row onwards.

Step 5 Enter a username and password. It is mandatory to fill the Username and Password fields in all the rows.

Step 6 Enter a profile. The Profile column if left blank (or filled in with *any profile*) means a client on any profile can use this account.

Step 7 Enter a description of the profile.

Step 8 Use the drop-down list to choose the SSID which this local user is applied to or choose the any SSID option.

Step 9 Enter a user-defined description of this interface. Skip to Step 11.

Step 10 If you want to override the existing template, select the **Override existing templates** check box.

Step 11 Click **Save**.

Guest User Templates

Choose **Configure > Controller Template Launch Pad > Security > Guest Users** to access the Guest Users list page.

Note To reduce clutter, the NCS does not show expired templates by default. You can specify which guest users to filter based on their status (active, scheduled, expired, not active, or none). Use the Select a Status Filter drop-down list to determine the filter criteria.

Note Click the **Edit View** link to add, remove, or reorder columns in the Guest Users table.

Configuring a Guest User Template

This page allows you to add a guest user template or make modifications to an existing guest user template. The purpose of a guest user account is to provide a user account for a limited amount of time. A Lobby Ambassador is able to configure a specific time frame for the guest user account to be active. After the specified time period, the guest user account automatically expires. See the "Creating Guest User Accounts" section on page 6-10 for further information on guest access.

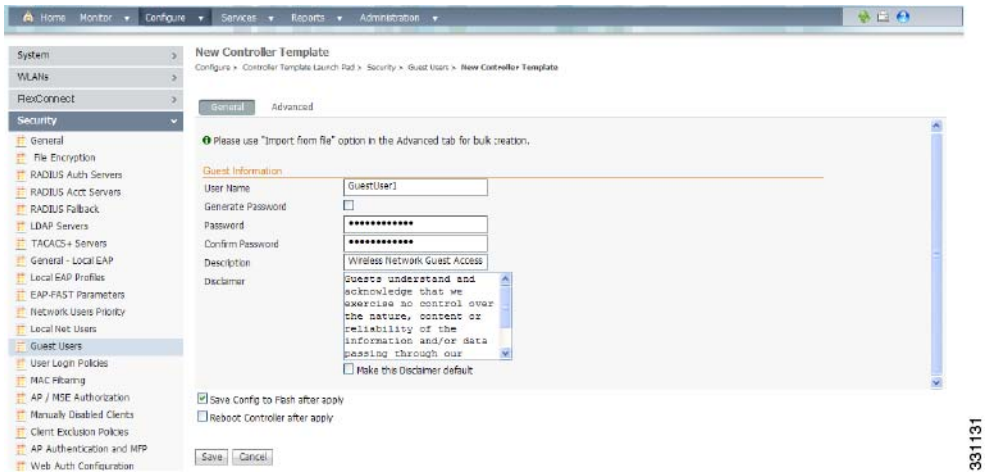
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Guest Users** or choose **Security > Guest Users** from the left sidebar menu.The Security > Guest User page appears.

Note To reduce clutter, the NCS does not show expired templates by default. You can specify which guest users to filter based on their status (active, scheduled, expired, not active, or none). Use the Select a Status Filter drop-down list to determine the filter criteria.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Guest Users template page appears (see Figure 10-29).

Figure 10-29 Guest User Template



Step 4 Enter a guest username in the User Name text box. The maximum size is 24 characters.

Step 5 Enter a password for this username in the Password text box.

Step 6 Click the **Advanced** tab.

Step 7 Use the Profile drop-down list to choose the guest user to connect to.

Step 8 Choose a user role for the guest user from the drop-down list. User roles are predefined by the administrator and are associated with the access of the guest (such as contractor, customer, partner, vendor, visitor, and so on).

User Role is used to manage the amount of bandwidth allocated to specific users within the network.

Step 9 Define how long the guest user account remains active by choosing either the Limited or Unlimited Lifetime option.

- For the limited option, you choose the period of time that the guest user account is active using the hours and minutes drop-down lists. The default value for Limited is one day (8 hours).
- When Unlimited is chosen, there is no expiration date for the guest account.

Step 10 Choose the area (indoor, outdoor), controller list, or config group to which the guest user traffic is limited from the Apply to drop-down list.

If you choose the controller list option, a list of controller IP addresses appears.

Step 11 (Optional) Modify the default guest user description on the General tab if necessary.

Step 12 (Optional) Modify the Disclaimer text on the General tab, if necessary. If you want the supplied text to be the default, select the **Make this Disclaimer default** check box.

Step 13 Click **Save**.

Configuring a User Login Policies Template

This page allows you to add a user login template or make modifications to an existing user login policies template. On this template you set the maximum number of concurrent logins that each single user can have.

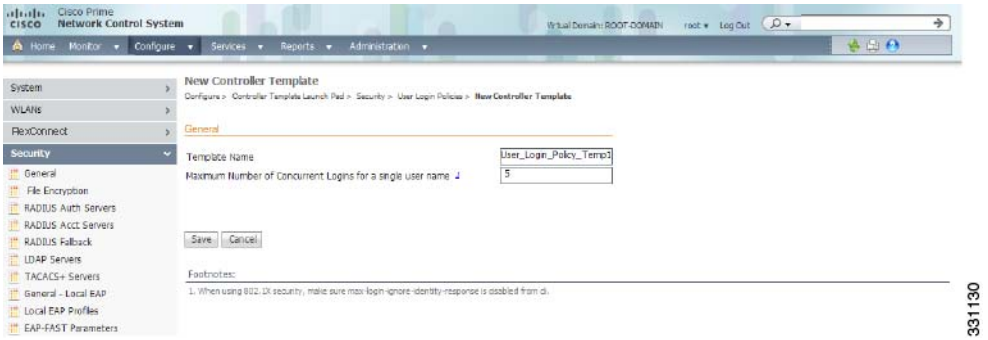
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **User Login Policies** or choose **Security > User Login Policies** from the left sidebar menu. The Security > User Login Policies page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The User Login Policies template page appears (see Figure 10-30).

Figure 10-30 User Login Policies Template



Step 4 You can adjust the maximum number of concurrent logins each single user can have.

Step 5 Click **Save** to keep this template.

Configuring a MAC Filter Template

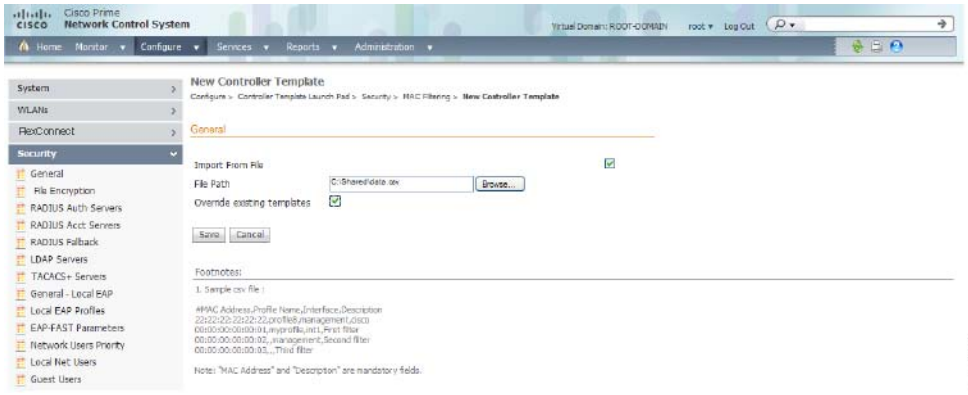
This page allows you to add a MAC filter template or make modifications to an existing MAC filter template.

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **MAC Filtering** or choose **Security > MAC Filtering** from the left sidebar menu. The Security > MAC Filtering page appears.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The MAC Filtering template page appears (see Figure 10-31).

Figure 10-31 MAC Filter Templates



Step 4 If you keep Import From File enabled, you must enter a file path or click **Browse** to navigate to the file path. The import file must be a CSV file with MAC address, profile name, interface, and description (such as 00:11:22:33:44:55, Profile1, management, test filter). If you unselect the Import from File check box, continue to Step 5. Otherwise, skip to Step 8.

The client MAC address appears.

Step 5 Choose the profile name to which this MAC filter is applied or choose the **any Profile** option.

Step 6 Use the drop-down list to choose from the available interface names.

Step 7 Enter a user-defined description of this interface. Skip to Step 9.

Step 8 If you want to override the existing template, select the **Override existing templates** check box.

Step 9 Click **Save**.

Note You cannot use MAC address in the broadcast range.

Configuring an Access Point or MSE Authorization Template

To add an MSE authorization or make changes to an existing access point or MSE authorization template, follow these steps:

Note These templates are devised for Cisco 11xx/12xx series access points converted from Cisco IOS to lightweight access points or for 1030 access points connecting in bridge mode. See the *Cisco Mobility Services Engine Configuration Guide* for further information.

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **AP/MSE Authorization** or choose **Security > AP/MSE Authorization** from the left sidebar menu. The Security > AP/LBS Authorization Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also shows the Base Radio MAC and the certificate type and key. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The AP/MSE Authorization template page appears (see Figure 10-32).

Figure 10-32 AP/MSE Authorization Templates

Step 4 Select the **Import From File** check box if you want to import a file containing access point MAC addresses.

Note You can only import a .csv file. The .csv file format parallels the fields in the GUI and therefore includes access point base radio MAC, Type, Certificate Type (MIC or SSC), and key hash (such as 00:00:00:00:00:00, AP, SSC, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx). Any other file formats are not supported.

Step 5 Enter the desired file path or click **Browse** to import the file.

Step 6 Click **Save**.

Note You cannot use MAC address in the broadcast range.

Configuring a Manually Disabled Client Template

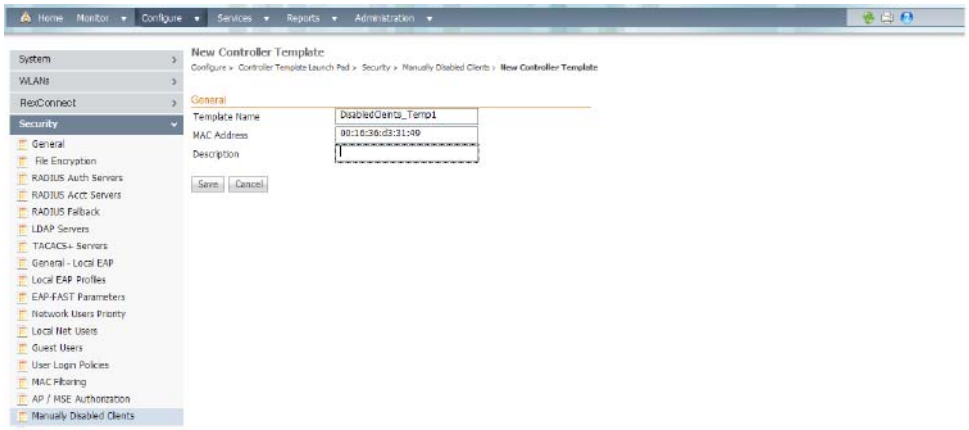
This page allows you to add a manually disable client template or make modifications to an existing disabled client template.

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Disable Clients** or choose **Security > Disabled Clients** from the left sidebar menu. The Security > Disabled Clients page appears.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Manually Disabled template page appears (see Figure 10-33).

Figure 10-33 Manually Disabled Clients Template



Step 4 Enter the MAC address of the client you want to disable.

Step 5 Enter a description of the client you are setting to disabled.

Step 6 Click **Save**.

Note You cannot use a MAC address in the broadcast range.

Configuring a Client Exclusion Policies Template

To add a client exclusion policies template or modify an existing client exclusion policies template, follow these steps:

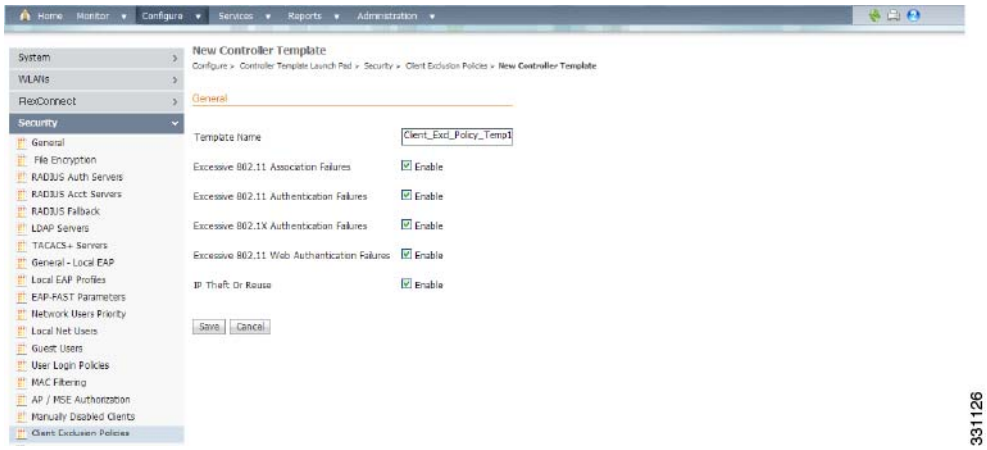
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Client Exclusion Policies** or choose **Security > Client Exclusion Policies** from the left sidebar menu. The Security > Client Exclusion Policies page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Client Exclusion Policies template page appears (see Figure 10-34).

Figure 10-34 Policies Template



Step 4 Edit a client exclusion policies template by configuring its field (see Table 10-3).

Table 10-3 Policies Template Fields

Field	Description
Template Name	Enter a name for the client exclusion policy.
Excessive 802.11 Association Failures	Enable to exclude clients with excessive 802.11 association failures.
Excessive 802.11 Authentication Failures	Enable to exclude clients with excessive 802.11 authentication failures.
Excessive 802.1X Authentication Failures	Enable to exclude clients with excessive 802.1X authentication failures.
Excessive 802.11 Web Authentication Failures	Enable to exclude clients with excessive 802.11 web authentication failures.
IP Theft or Reuse	Enable to exclude clients exhibiting IP theft or reuse symptoms.

Step 5 Click **Save**.

Configuring an Access Point Authentication and MFP Template

Management Frame Protection (MFP) provides for the authentication of 802.11 management frames by the wireless network infrastructure. Management frames can be protected to detect adversaries who are invoking denial of service attacks, flooding the network with associations and probes, interjecting as rogue access points, and affecting the network performance by attacking the QoS and radio measurement frames.

When enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving access point configured to detect MFP frames to report the discrepancy. An access point must be a member of a WDS to transmit MFP frames.

When MFP detection is enabled, the access point validates every management frame that it receives from other access points in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an access point that is configured to transmit MFP frames, it reports the discrepancy to the network management system.

To add or make modifications for the access point authentication and management frame protection (MFP) template, follow these steps:

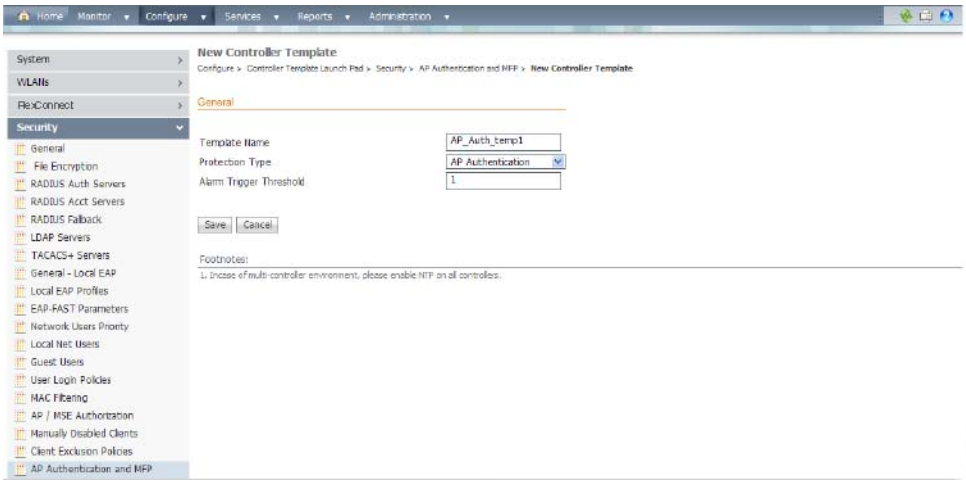
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **AP Authentication and MFP** or choose **Security > AP Authentication and MFP** from the left sidebar menu. The Security > AP Authentication Policy Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The AP Authentication and MFP template page appears (see Figure 10-35).

Figure 10-35 AP Authentication Policy Template



Step 4 From the Protection Type drop-down list, choose one of the following authentication policies:

- **None**—No access point authentication policy.
- **AP Authentication**—Apply authentication policy.
- **MFP**—Apply management frame protection.

Alarm trigger threshold appears only when AP authentication is selected as a protection type. Set the number of hits from an alien access point to ignore before raising an alarm.

The valid range is from 1 to 255. The default value is 255.

Step 5 Click **Save**.

Configuring a Web Authentication Template

With web authentication, guests are automatically redirected to a web authentication page when they launch their browsers. Guests gain access to the WLAN through this web portal. Wireless LAN administrators using this authentication mechanism should have the option of providing unencrypted or encrypted guest access. Guest users can then log into the wireless network using a valid username and password, which is encrypted with SSL. Web authentication accounts might be created locally or managed by a RADIUS server. The Cisco Wireless LAN controllers can be configured to support a web authentication client. You can use this template to replace the Web authentication page provided on the controller.

To add or make modifications to an existing web authentication template, follow these steps:

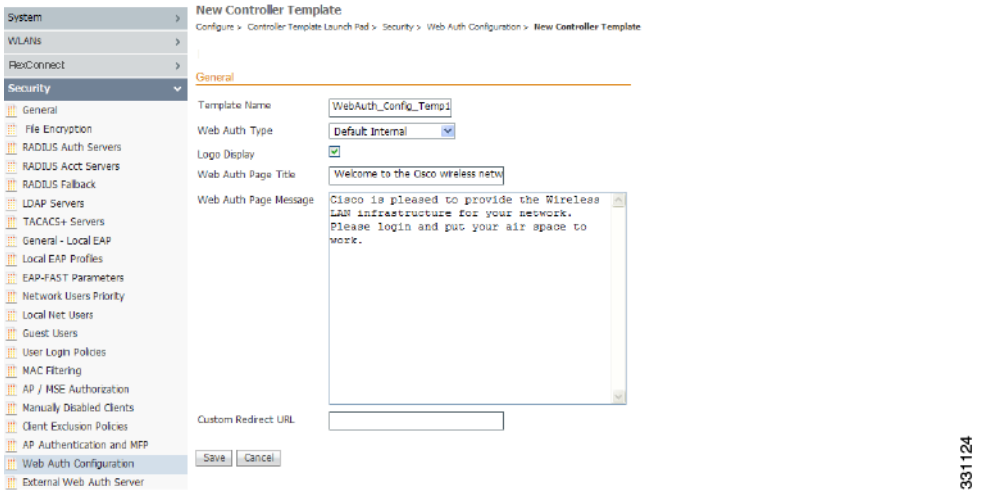
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Web Auth Configuration** or choose **Security > Web Auth Configuration** from the left sidebar menu. The Security > Web Authentication page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Web Authentication template page appears (see Figure 10-36).

Figure 10-36 Web Authentication Configuration Template



Step 4 Choose the appropriate web authentication type from the drop-down list. The choices are **default internal**, **customized web authentication**, or **external**.

- If you choose default internal, you can still alter the page title, message, and redirect URL, as well as whether the logo appears. Continue to Step 5.
- If you choose customized web authentication, click **Save** and apply this template to the controller. You are prompted to download the web authentication bundle.

Note Before you can choose customized web authentication, you must first download the bundle by going to **Config > Controller** and choose **Download Customized Web Authentication** from the Select a command drop-down list, and click **Go**.

- If you choose external, you need to enter the URL you want to redirect to after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page.

Step 5 Select the **Logo Display** check box if you want your company logo displayed.

Step 6 Enter the title you want displayed on the Web Authentication page.

Step 7 Enter the message you want displayed on the Web Authentication page.

Step 8 Provide the URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user would be directed to the company home page.

Step 9 Click **Save**.

Downloading a Customized Web Authentication Page

You can download a customized Web Authentication page to the controller. With a customized web page, you can establish a username and password for user web access.

When downloading customized web authentication, you must follow these strict guidelines:

- Provide a username.
- Provide a password.
- Retain a redirect URL as a hidden input item after extracting from the original URL.
- Extract the action URL and set aside from the original URL.
- Include scripts to decode the return status code.

Before downloading, follow these steps:

Step 1 Download the sample login.html bundle file from the server. The .html file is shown in Figure 10-37. The login page is presented to web users the first time they access the WLAN if web authentication is turned on.

Figure 10-37 Login.html

Step 2 Edit the login.html file and save it as a .tar or .zip file.

Note You can change the text of the Submit button to read Accept terms and conditions and Submit.

Step 3 Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable. However, if you want to put the TFTP server on a different network while the management port is down, add a static route if the subnet where the service port resides has a gateway (config route add *IP address of TFTP server*).
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the NCS because the built-in TFTP server of the NCS and third-party TFTP server use the same communication port.

Step 4 Download the .tar or .zip file to the controller(s).

Note The controller allows you to download up to 1 MB of a .tar file containing the pages and image files required for the Web authentication display. The 1 MB limit includes the total size of uncompressed files in the bundle.

You can now continue with the download.

Step 5 Copy the file to the default directory on your TFTP server.

Step 6 Choose **Configure > Controllers**.

Step 7 Choose a controller by clicking the URL for the corresponding IP address. If you select more than one IP address, the customized Web authentication page is downloaded to multiple controllers.

Step 8 From the left sidebar menu, choose **System > Commands**.

Step 9 From the Upload/Download Commands drop-down list, choose **Download Customized Web Auth,** and click **Go**.

Step 10 The IP address of the controller to receive the bundle and the current status are displayed.

Step 11 Choose **local machine** from the File is Located On field. If you know the filename and path relative to the root directory of the server, you can also select TFTP server.

Note For a local machine download, either .zip or .tar file options exists, but the NCS does the conversion of .zip to .tar automatically. If you chose a TFTP server download, only .tar files would be specified.

Step 12 Enter the maximum number of times the controller should attempt to download the file in the Maximum Retries field.

Step 13 Enter the maximum amount of time in seconds before the controller times out while attempting to download the file in the Timeout field.

Step 14 The files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** to navigate to it.

Step 15 Click **OK**.

If the transfer times out, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you. The local machine option initiates a two-step operation. First, the local file is copied from the workstation of the administrator to the built-in TFTP server of the NCS. Then the controller retrieves that file. For later operations, the file is already in the TFTP directory of the NCS server, and the download web page now automatically populates the filename.

Step 16 Click the **Click here to download a sample tar file** link to get an option to open or save the login.tar file.

Step 17 After completing the download, you are directed to the new page and able to authenticate.

Configuring an External Web Auth Server Template

To create or modify an External Web Auth Server template, follow these steps:

Step 1 Choose **Configure > Controller Templates Launch Pad**.

Step 2 Click **External Web Auth Server** or choose **Security > External Web Auth Server** from the left sidebar menu. The External Web Auth Server Controller Templates page displays all currently saved External Web Auth Server templates. It also displays the number of controllers and virtual domains to which each template is applied.

Step 3 Click a template name to open the Controller Template list page. In this page, you can edit the current template fields.

Configuring a Security Password Policy Template

This page enables you to determine your security password policy.

To add or make modifications to an existing password policy template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Password Policy** or choose **Security > Password Policy** from the left sidebar menu. The Security > Password Policy page appears.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Password Policy template page appears (see Figure 10-38).

Figure 10-38 Password Policy Template

Step 4 Enter the template name.

Step 5 You can enable or disable the following settings:

- Password must contain characters from at least 3 different classes such as uppercase letters, lowercase letters, digits, and special characters.
- No character can be repeated more than 3 times consecutively.
- Password cannot be the default words like cisco, admin.

Note Password cannot be “cisco”, “ocsic”, “admin”, “nimda’ or any variant obtained by changing the capitalization of letters, or by substituting ‘1” “|” or “!” for i, or substituting “0” for “o”, or substituting “$” for “s”.

- Password cannot contain username or reverse of username.

Step 6 Click **Save**.

Configuring Security - Access Control Templates

This section contains the following topics:

Configuring an Access Control List Template

You can create or modify an ACL template for configuring the type of traffic that is allowed, by protocol, direction, and the source or destination of the traffic.

An access control list (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). ACLs can be applied to data traffic to and from wireless clients or to all traffic destined for the controller Central Processing Unit (CPU) and can now support reusable grouped IP addresses and reusable protocols. After ACLs are configured in the template, they can be applied to the management interface, the AP-manager interface, or any of the dynamic interfaces for client data traffic; to the Network Processing Unit (NPU) interface for traffic to the controller CPU; or to a WAN.

This release of the NCS provides support to IPv6 ACLs.

To add or modify an existing ACL template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Access Control Lists** or choose **Security > Access Control > Access Control Lists** in the left sidebar menu. The Security > Access Control List page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new Access Control List template, choose **Add Template** from the Select a command drop-down list, and click **Go**. The New Controller Template page appears. In this page, specify the following fields:

- Access Control List Name—User-defined name of the template.
- ACL Type—Choose either **IPv4** or **IPv6**.

Note IPv6 ACL is supported from controller Release 7.2.x.

Step 4 To create reusable grouped IP addresses and protocols, choose **Access Control > IP Groups** from the left sidebar menu.

Step 5 All the IP address groups are listed. One IP address group can have a maximum of 128 IP address and netmask combinations. To define a new IP address group, choose **Add IP Group** from the Select a command drop-down list, and click **Go**. To view or modify an existing IP address group, click the URL of the IP address group. The IP address group page opens.

Note For the IP address of any, an *any* group is predefined.

Step 6 In the ACL IP Groups details page you can edit the current IP group fields.

- IP Group Name
- IP Address
- Netmask OR CIDR Notation—Enter the Netmask or CIDR Notation and then click **Add**. The list of IP addresses or Netmasks appears in the List of IP Address/Netmasks text box.

CIDR notation allows you to add a large number of clients that exist in a subnet range by configuring a single client object.

Netmask allows you to set the subnet mask in dotted-decimal notation rather than the CIDR notation for the IP address property.

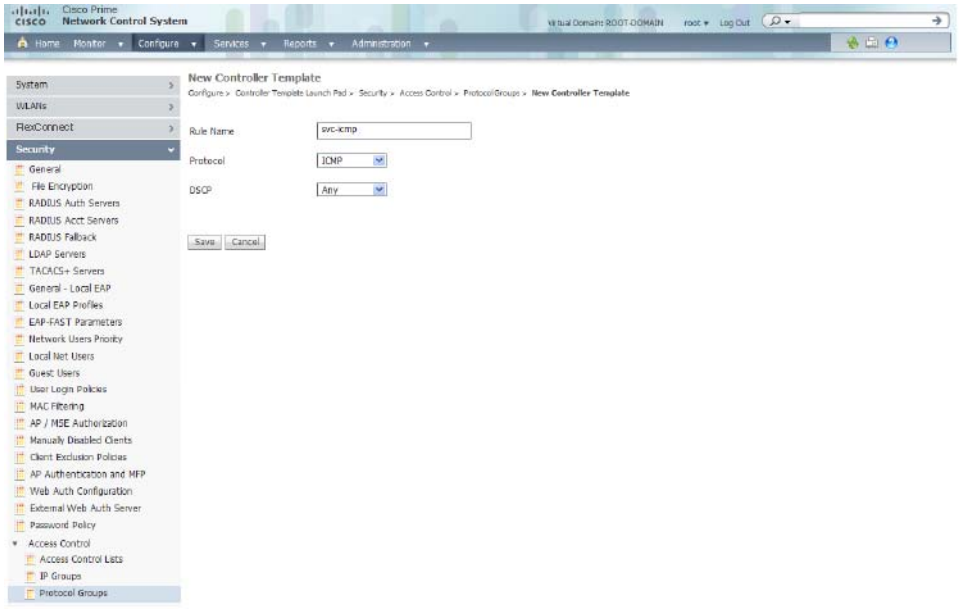
- Netmask—A range of IP addresses defined so that only machines with IP addresses within the range are allowed to access an Internet service.
- CIDR—Classless InterDomain Routing. A protocol which allows the assignment of Class C IP addresses in multiple contiguous blocks.

- BroadCast/Network
- List of IP Addresses/Netmasks—Use the Move Up and Move Down buttons to rearrange the order of the list items. Use the Delete button to delete any IP address or Netmask.

Step 7 To define an additional protocol that is not a standard predefined one, choose **Access Control > Protocol Groups** from the left sidebar menu. The protocol groups with their source and destination port and DSCP are displayed.

Step 8 To create a new protocol group, choose **Add Protocol Group** from the Select a command drop-down list, and click **Go**. To view or modify an existing protocol group, click the URL of the group. The Protocol Groups page appears (see Figure 10-39).

Figure 10-39 Protocol Groups Controller Template



Step 9 The rule name is provided for the existing rules, or you can now enter a name for a new rule. ACLs are not required to have rules defined. When a packet matches all the parameters of a rule, the action for this rule is exercised.

Step 10 Choose a protocol from the drop-down list:

- Any—All protocols
- TCP—Transmission Control Protocol
- UDP—User Datagram Protocol
- ICMP—Internet Control Message Protocol

- ESP—IP Encapsulating Security Payload
- AH—Authentication Header
- GRE—Generic Routing Encapsulation
- IP—Internet Protocol
- Eth Over IP—Ethernet over Internet Protocol
- Other Port OSPF—Open Shortest Path First
- Other—Any other IANA protocol (http://www.iana.org/)

Step 11 Some protocol choices (such as TCP or UDP) cause additional Source Port and Dest Port GUI elements to appear.

- Source Port—Specify the source of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.
- Dest Port—Specify the destination of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.

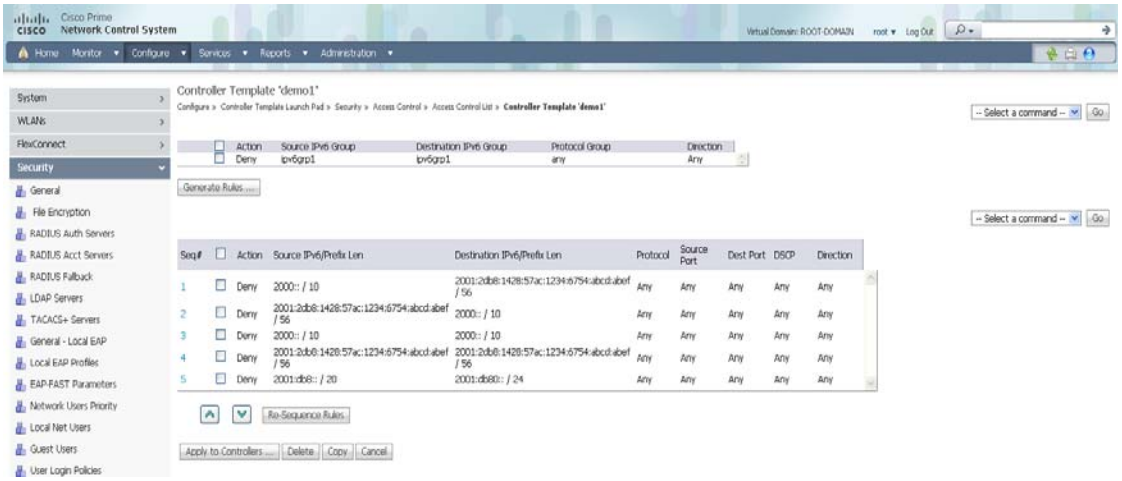
Step 12 From the DSCP (Differentiated Services Code Point) drop-down list, choose **any** or **specific**. If you choose specific, enter the DSCP (range of 0 to 255).

Note DSCP is a packet header code that can be used to define the quality of service across the Internet.

Step 13 Click **Save**.

Step 14 You can now create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All ACL mappings appear on the top of the page, and all ACL rules appear on the bottom (see Figure 10-40).

Figure 10-40 Access Control List Rule Mapping



Step 15 To define a new mapping, choose **Add Rule Mappings** from the Select a command drop-down list. The Add Rule Mapping page appears.

Step 16 Configure the following fields:

- Source IP Group—Predefined groups for IPv4 and IPv6.
- Destination IP Group—Predefined groups for IPv4 and IPv6.
- Protocol Group—Protocol group to use for the ACL.
- Direction—Any, Inbound (from client) or Outbound (to client).
- Action—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.

Step 17 Click **Add**. The new mappings populate the bottom table.

Step 18 Click **Save**.

Step 19 You can now automatically generate rules from the rule mappings you created. Choose the mappings for which you want to generate rules, and click **Generate**. This automatically creates the rules. These rules are generated with contiguous sequence. That is, if rules 1 through 4 are already defined and you add rule 29, it is added as rule 5.

Existing ACL templates are duplicated into a new ACL template. This duplication clones all the ACL rules and mappings defined in the source ACL template.

Configuring a FlexConnect Access Control List Template

You can create or modify a FlexConnect ACL template for configuring the type of traffic that is allowed by protocol, and the source or destination of the traffic.

Note The FlexConnect ACLs do not support IPv6 addresses.

This section contains the following topics:

- Configuring and Applying a FlexConnect Access Control List, page 10-76
- Deleting a FlexConnect Access Control List, page 10-77

Configuring and Applying a FlexConnect Access Control List

To configure and apply an Access Control List template to a Controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **Security > Access Control > FlexConnect ACLs**.

Step 4 From the Select a command drop-down list, choose **Add a Template**.

Step 5 Click **Go**.

The New Controller Template page appears.

Step 6 Enter a name for the new FlexConnect ACL in the **FlexConnect ACL Name** text box.

Step 7 Click **Save**.

A FlexConnect ACL template is created. You can now create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All FlexConnect ACL mappings appear on the top of the page, and all FlexConnect ACL rules appear in the bottom.

Step 8 From the Select a command drop-down list, choose **Add Rule Mappings**, and click **Go**.

Step 9 The FlexConnect ACL IP Protocol Map page appears.

Step 10 Configure the following fields:

- Source IP Group—Predefined groups for IPv4 and IPv6.
- Destination IP Group—Predefined groups for IPv4 and IPv6.
- Protocol Group—Protocol group to use for the ACL.
- Action—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.

Step 11 Click **Add**. The new mappings populate the bottom table.

Step 12 Click **Save**.

Step 13 You can now automatically generate rules from the rule mappings you created. Choose the mappings for which you want to generate rules, and click **Generate**. This automatically creates the rules. These rules are generated with contiguous sequence. That is, if rules 1 through 4 are already defined and you add rule 29, it is added as rule 5.

Existing FlexConnect ACL templates are duplicated into a new FlexConnect ACL template. This duplication clones all the FlexConnect ACL rules and mappings defined in the source FlexConnect ACL template.

Step 14 From the Select a command drop-down list in the FlexConnect ACL page, choose **Apply Templates**.

The Apply to Controllers page appears.

Step 15 Select **Save Config to Flash after apply** check box to save the configuration to Flash after applying the FlexConnect ACL to the controller.

Step 16 Select **Reboot Controller after apply** to reboot the controller once the FlexConnect ACL is applied. This check box is available only when you select the Save Config to Flash after apply check box.

Step 17 Select one or more controllers and click **OK** to apply the FlexConnect ACL template.

The FlexConnect ACL that you created appears in Configure > Controller Template Launch Pad > <*IP Address*> > Security > Access Control > FlexConnect ACLs.

Deleting a FlexConnect Access Control List

To delete a FlexConnect ACL, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **Security > FlexConnect ACLs**.

Step 4 From the FlexConnect ACLs page, select one or more FlexConnect ACLs to delete.

Step 5 From the Select a command drop-down list, choose **Delete FlexConnect ACLs**.

Step 6 Click **Go**.

Configuring an ACL IP Groups Template

To create reusable grouped IP addresses, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Choose **Security > Access Control > IP Groups** from the left sidebar menu.

Step 3 All the IP address including IPv4 and IPv6 groups are listed. One IP address group can have a maximum of 128 IP address and netmask combinations. To define a new IP address group, choose **Add IP Group or Add IPv6 Group** from the Select a command drop-down list, and click **Go**.

Note For the IP address of any, an *any* group is predefined.

Note For the IPv6 address of any, an *any* group is predefined with an IP address type as IPv6.

Step 4 Configure the following fields:

- IP Group Name
- IP Address—For IP Group, enter an IPv4 address format. For IPv6 groups, enter an IPv6 address format.
- Netmask OR CIDR Notation—Enter the Netmask or CIDR Notation and then click **Add**. The list of IP addresses or Netmasks appears in the List of IP Addresses/Netmasks text box.

  Note These fields are not applicable for IPv6 groups.

  CIDR notation allows the user to add a large number of clients that exist in a subnet range by configuring a single client object.

  Netmask allows the user to set the subnet mask in dotted-decimal notation rather than the CIDR notation for the IP address property.

  - Netmask—A range of IP addresses defined so that only machines with IP addresses within the range are allowed to access an Internet service.
  - CIDR—Classless InterDomain Routing. A protocol which allows the assignment of Class C IP addresses in multiple contiguous blocks.
- BroadCast/Network

  Note These fields are not applicable for IPv6 groups.

- Prefix Length—Prefix for IPv6 addresses, ranging from 0 to 128.
- List of IP Addresses/Netmasks—Use the Move Up and Move Down buttons to rearrange the order of the list items. Use the Delete button to delete an IP address or Netmask.

Step 5 Click **Save**. Once saved, the IP Group appears in the Template List page.

You can create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All ACL mappings appear in the top of the page, and all ACL rules appear in the bottom. See the "Configuring an Access Control List Template" section on page 10-73 for more information.

See the "Configuring an ACL Protocol Groups Template" section on page 10-79 for information on defining Protocol Groups.

Configuring an ACL Protocol Groups Template

To define an additional protocol that is not a standard predefined one, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Choose **Access Control > Protocol Groups** from the left sidebar menu.

Step 3 Configure the following fields:

- Rule Name—The rule name is provided for the existing rules, or you can now enter a name for a new rule. ACLs are not required to have rules defined. When a packet matches all the fields of a rule, the action for this rule is exercised.

  Note See the "Configuring an Access Control List Template" section on page 10-73 for more information on ACLs.

- Protocol—Choose a protocol from the drop-down list:
  - Any—All protocols
  - TCP—Transmission Control Protocol
  - UDP—User Datagram Protocol
  - ICMP—Internet Control Message Protocol
  - ESP—IP Encapsulating Security Payload
  - AH—Authentication Header
  - GRE—Generic Routing Encapsulation
  - IP—Internet Protocol
  - Eth Over IP—Ethernet over Internet Protocol
  - Other Port OSPF—Open Shortest Path First
  - Other—Any other IANA protocol (http://www.iana.org/)
- Source Port—Can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
- Dest Port—Destination port. If TCP or UDP is selected, can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
- DSCP (Differentiated Services Code Point)—Choose Any or Specific from the drop-down list. If Specific is selected, enter the DSCP (range of 0 through 255).

  Note DSCP is a packet header code that can be used to define the quality of service across the Internet.

Step 4 Click **Save**. Once saved, the IP Group displays in the Template List page.

You can create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All ACL mappings appear in the top of the page, and all ACL rules appear in the bottom. See the "Configuring an Access Control List Template" section on page 10-73 for more information.

See the "Configuring an ACL IP Groups Template" section on page 10-78 for information on defining IP Groups.

Configuring Security - CPU Access Control List Templates

Note CPU ACL configuration with IPv6 is not supported in this release becuase all IP addresses of controllers on interfaces use IPv4 except the virtual interface.

Configuring a CPU Access Control List (ACL) Template

The existing ACLs established in the "Configuring an Access Control List Template" section on page 10-73 is used to set traffic controls between the Central Processing Unit (CPU) and Network Processing Unit (NPU).

To add or modify an existing CPU ACL template, follow these steps:

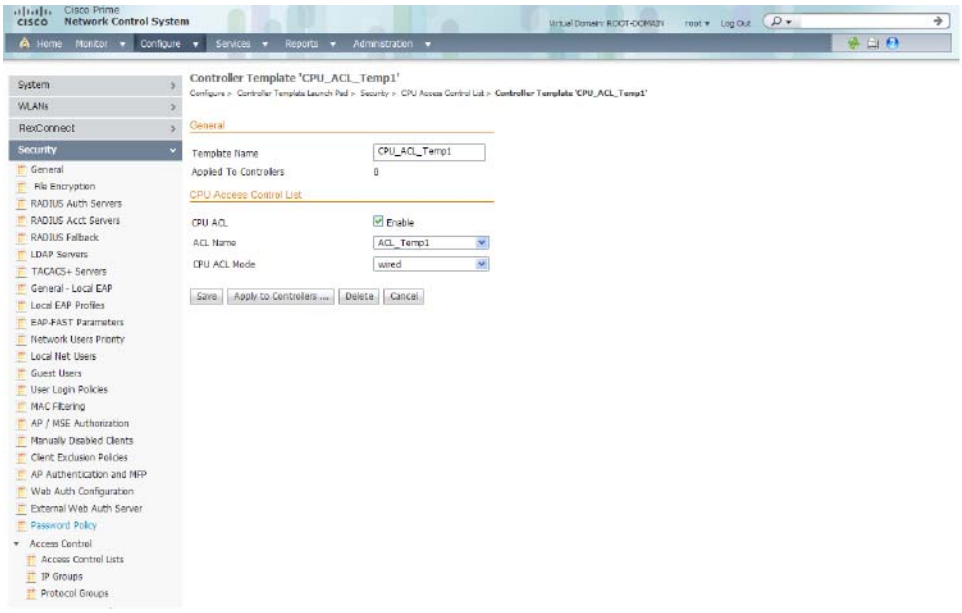
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **CPU Access Control Lists** or choose **Security > CPU Access Control > CPU Access Control List** from the left sidebar menu. The Security > CPU Access Control List page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The CPU Access Control List template page appears (see Figure 10-41).

Figure 10-41 CPU Access Control List Template



Step 4 If you select the check box to enable CPU ACL, two more fields appear. When CPU ACL is enabled and applied on the controller, the NCS displays the details of the CPU ACL against that controller.

Step 5 From the ACL Name drop-down list, choose a name from the list of defined names.

Step 6 From the CPU ACL Mode drop-down list, choose which data traffic direction this CPU ACL list controls. The choices are the wired side of the data traffic, the wireless side of the data traffic, or both wired and wireless.

Step 7 Click **Save**.

Configuring Security - Rogue Templates

This section contains the following topics:

Configuring a Rogue Policies Template

This page enables you to configure the rogue policy (for access points and clients) applied to the controller.

To add or modify an existing template, follow these steps:

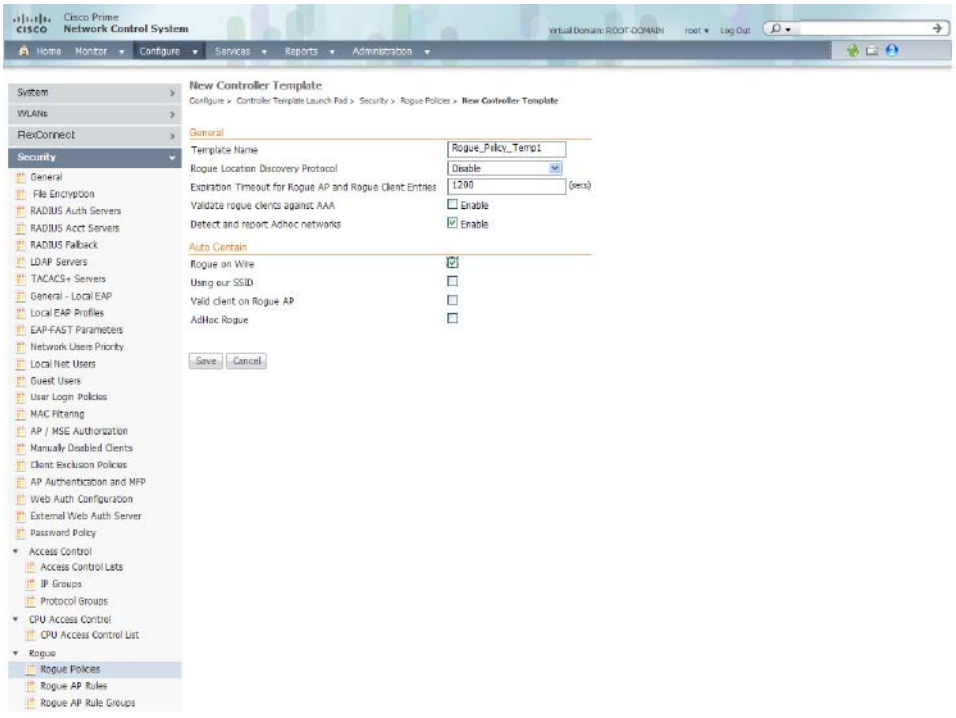
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Rogue Policies** or choose **Security > Rogue > Rogue Policies** from the left sidebar menu. The Security > Rogue Policy Setup page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Rogue Policies template page appears (see Figure 10-42).

Figure 10-42 Rogue Policy Setup Template



Step 4 Determine whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network. Choose one of the following from the drop-down list:

- **Disable**—Disables RLDP on all access points.
- **All APs**—Enables RLDP on all access points.
- **Monitor Mode APs**—Enables RLDP only on access points in monitor mode.

Note With RLDP, the controller instructs a managed access point to associate with the rogue access point and sends a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points that do not have encryption enabled.

Step 5 Set the expiration timeout (in seconds) for rogue access point entries.

Step 6 In the Rogue Detection Report Interval text box, enter the time interval in seconds at which the APs should send the rogue detection report to the controller. A valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.

Step 7 In the Rogue Detection Minimum RSSI text box, enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. A valid range is -70 dBm to -128 dBm, and the default value is -128 dBm. This feature is applicable to all the AP modes.

Note There can be many rogues with very weak RSSI values that do not provide any valuable information in the rogue analysis. Therefore, you can use this option to filter the rogues by specifying the minimum RSSI value at which the APs should detect rogues.

Step 8 In the Rogue Detection Transient Interval text box, enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only.

Step 9 Select the **Validate rogue clients against AAA** check box to enable the AAA validation of rogue clients.

Step 10 Select the **Detect and report Adhoc networks** check box to enable detection and reporting of rogue clients participating in ad hoc networking.

Step 11 Click **Save**.

Configuring a Rogue AP Rules Template

Rogue access point rules allow you to define rules to automatically classify rogue access points. The NCS applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

Note Rogue access point rules also help reduce false alarms.

To view current classification rule templates, rule type, and the number of controllers to which they are applied, choose **Configure > Controller Template Launch Pad> Security > Rogue > Rogue AP Rules**. If you want to view rogue access point rules, see the "Viewing or Editing Rogue Access Point Rules" section on page 8-199.

Note Rogue classes include the following types:
Malicious Rogue—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly AP category.
Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.
Unclassified Rogue—A detected access point that does not match the malicious or friendly rules.

To add or create a new classification rule template for rogue access points, follow these steps:

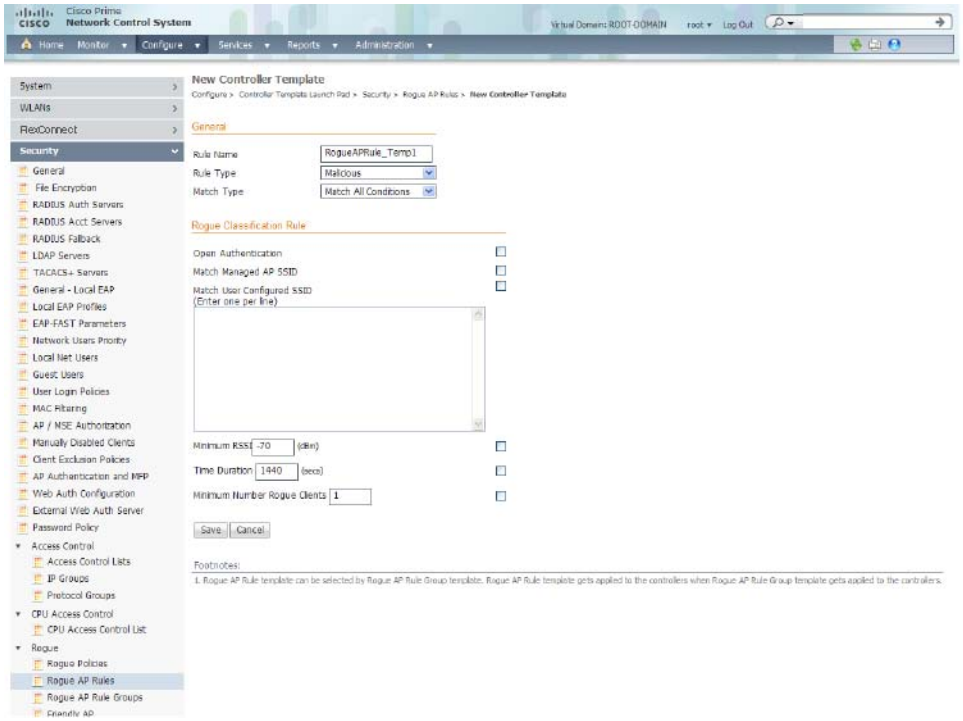
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 From the left sidebar menu, choose **Security > Rogue > Rogue AP Rules**. The Rogue AP Rules Controller template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 From the Select a command drop-down list, choose **Add Classification Rule**, and click **Go**. The Rogue AP Rules > New Template page appears (see Figure 10-43). To modify an existing rogue access point rules template or to apply a current template to the controllers, choose **Configure > Controller Template Launch Pad > Security > Rogue > Rogue AP Rules**, and click a template name.

Figure 10-43 Rogue AP Rules > New Template Page



Step 4 In the General group box, configure the following fields:

- Rule Name—Enter a name for the rule in the text box.
- Rule Type—Choose **Malicious** or **Friendly** from the drop-down list. A rogue is considered malicious if a detected access point matches the user-defined malicious rules or has been manually moved from the Friendly AP category. A rogue is considered friendly if it is a known, acknowledged, or trusted access point or a detected access point that matches the user-defined Friendly rules.
- Match Type—Choose **Match All Conditions** or **Match Any Condition** from the drop-down list.

Step 5 In the Malicious Rogue Classification Rule group box of the page, configure the following fields.

- Open Authentication—Select the check box to enable open authentication.

- Match Managed AP SSID—Select the check box to enable the matching of a Managed AP SSID.

  Note Managed SSIDs are the SSIDs configured for the WLAN and known to the system.

- Match User Configured SSID—Select the check box to enable the matching of User Configured SSIDs.

  Note User Configured SSIDs are the SSIDs that are manually added. Enter the User Configured SSIDs (one per line) in the Match User Configured SSID text box.

- Minimum RSSI—Select the check box to enable the Minimum RSSI threshold limit.

  Note Enter the minimum RSSI threshold level (dB) in the text box. The detected access point is classified as malicious if it is detected above the indicated RSSI threshold.

- Time Duration—Select the check box to enable the Time Duration limit.

  Note Enter the time duration limit (in seconds) in the text box. The detected access point is classified as malicious if it is viewed for a longer period of time than the indicated time limit.

- Minimum Number Rogue Clients—Select the check box to enable the Minimum Number Rogue Clients limit. Enter the minimum number of rogue clients allowed. The detected access point is classified as malicious if the number of clients associated to the detected access point is greater than or equal to the indicated value.

Step 6 Click **Save**.

Configuring a Rogue AP Rule Groups Template

A rogue access point rule group template allows you to combine more than one rogue access point rule to controllers.

To view current rogue access point rule group templates or create a new rule group, follow these steps:

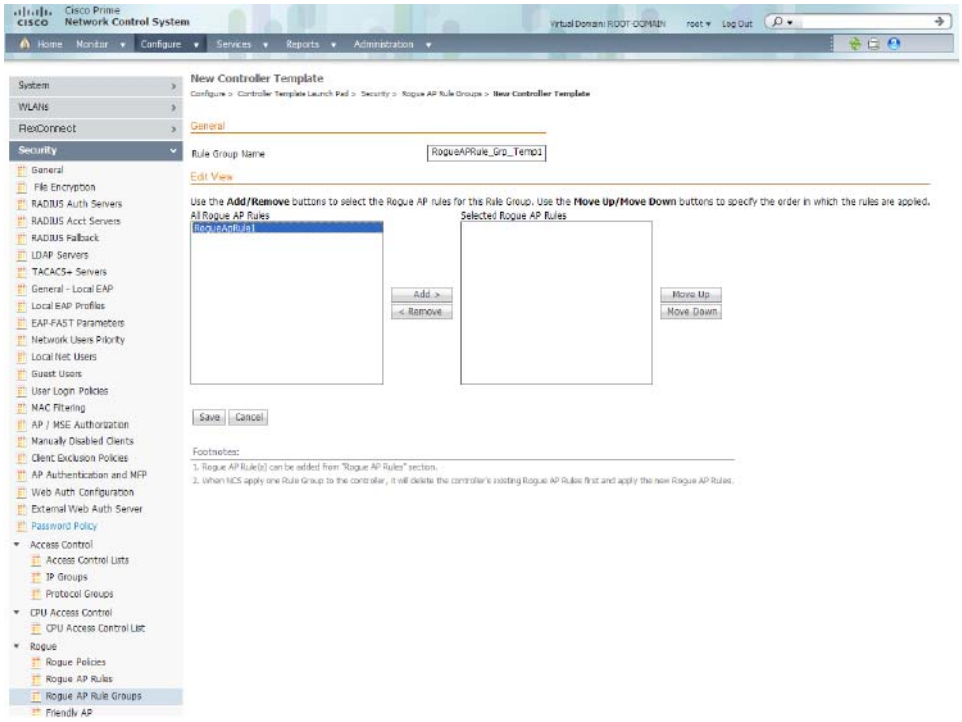
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Rogue AP Rule Groups** or choose **Security > Rogue > Rogue AP Rule Groups** from the left sidebar menu.

Step 3 From the Select a command drop-down list, click **Add Rogue Rule Group**.

Step 4 Click **Go**. The Rogue AP Rule Groups > New Template page appears (see Figure 10-44).

Figure 10-44 Rogue AP Rule Groups > New Template



Note To modify an existing rogue policy template or to apply a current template to controllers, choose **Configure > Controller Template Launch Pad > Security > Rogue > Rogue AP Rule Groups** and click a template name. Make the necessary changes to the template, and click **Save** or **Apply to Controllers**.

Step 5 Enter a name for the rule group in the General group box of the page.

Step 6 To add a Rogue AP rule, click to highlight the rule in the left column. Click **Add** to move the rule to the right column.

Note Rogue access point rules can be added from the Rogue Access Point Rules section. See the "Configuring a Rogue AP Rules Template" section on page 10-83 for more information.

Step 7 To remove a rogue access point rule, click to highlight the rule in the right column. Click **Remove** to move the rule to the left column.

Step 8 Use the **Move Up/Move Down** buttons to specify the order in which the rules apply. Highlight the desired rule and click **Move Up** or **Move Down** to move it higher or lower in the current list.

Step 9 Click **Save** to confirm the rogue access point rule list.

Step 10 Click **Cancel** to close the page without making any changes to the current list.

Note To view and edit the rules applied to a controller, choose **Configure > Controller**, and click the controller name.

Configuring a Friendly Access Point Template

This template allows you to import friendly internal access points. Importing these friendly access points prevents non-lightweight access points from being falsely identified as rogues.

Note *Friendly Internal* access points were previously referred to as *Known APs*.

Note The Friendly AP page identifies the MAC address of an access point, status, any comments, and whether or not the alarm is suppressed for this access point.

To view or edit the current list of friendly access points, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

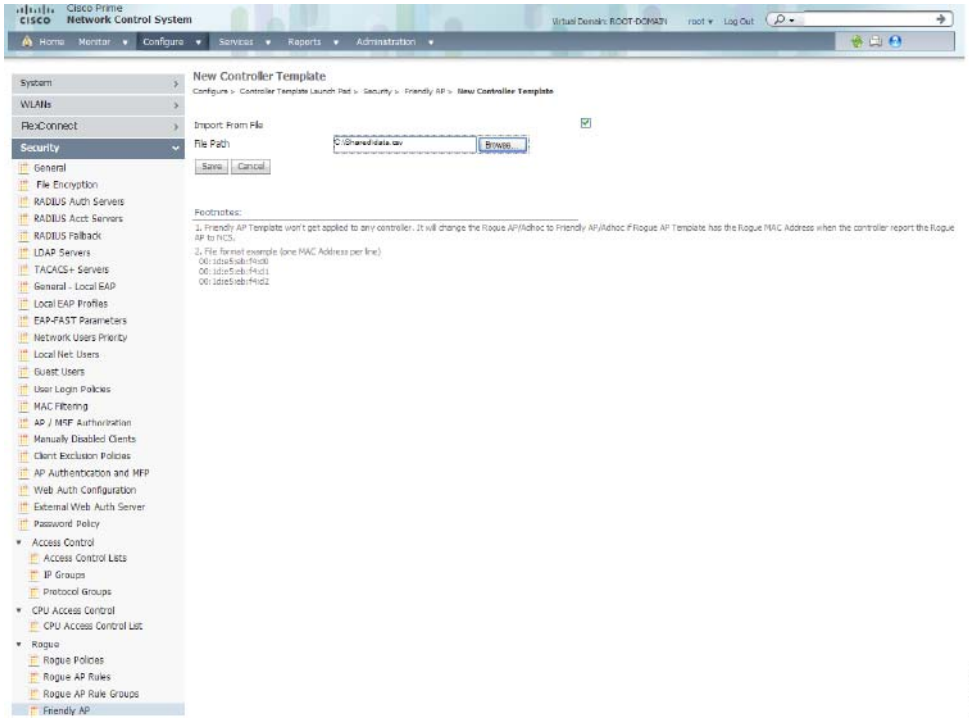
Step 2 Click **Friendly AP** or choose **Security > Rogue > Friendly AP** from the left sidebar menu.

Step 3 From the Select a command drop-down list, choose **Add Friendly**.

Step 4 Click **Go**. The Friendly AP page appears (see Figure 10-45).

Note To modify an existing friendly access point, choose **Configure > Controller Template Launch Pad > Security > Rogue > Friendly Internal**, and click the MAC address of an access point. Make the necessary changes to the access point, and click **Save**.

Figure 10-45 Friendly AP > Add Friendly AP Page



Step 5 Friendly access points can be added by either importing the access point or manually entering the access point information:

- To import an access point using the Import feature do the following:
  - Select the **Import from File** check box.
  - Enter the file path or click **Browse** to navigate to the correct file.

  Note Use a line break to separate MAC addresses. For example, enter the MAC addresses as follows:
  00:00:11:22:33:44
  00:00:11:22:33:45
  00:00:11:22:33:46

- To manually add an access point, do the following:
  - Unselect the **Import from File** check box.
  - Enter the MAC address for the access point.
  - Choose **Internal** access point from the Status drop-down list.
  - Enter a comment regarding this access point, if necessary.
  - Select the **Suppress Alarms** check box to suppress all alarms for this access point.
- Click **Save** to confirm this access point or **Cancel** to close the page without adding the access point to the list.

Configuring Ignored Rogue AP Templates

The Ignored Rogue AP Template page allows you to create or modify a template for importing ignored access points. Access points in the Ignored AP list are not identified as rogues.

Note An Ignored Rogue AP template does not get applied to any controller. It suppresses the Rogue AP/Adhoc alarm if Ignored Rogue AP Template has the Rogue MAC Address when the controller reports the Rogue AP to the NCS and this MAC address is added to the Rogue AP Ignore-List on the controller.

To add or edit the Ignored Rogue access points, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Ignored Rogue AP** or choose **Security > Rogue > Ignored Rogue AP** from the left sidebar menu.

Step 3 From the Select a command drop-down list, choose **Add Ignored Rogue AP**.

Step 4 Click **Go**. The Ignored Rogue AP page appears.

Step 5 The Ignored Rogue access points can be added by either importing the access point or manually entering the access point information:

- To import an ignored rogue access point using the Import feature:
  - Select the **Import from File** check box.
  - Enter the file path or use the **Browse** button to navigate to the correct file. The import file must be a CSV file with MAC address (one MAC Address per line).

    Note For example, enter the MAC addresses as follows:
    00:00:11:22:33:44
    00:00:11:22:33:45
    00:00:11:22:33:46

- To manually add an ignored rogue access point:
  - Unselect the **Import from File** check box.
  - Enter the MAC address and comment for the rogue access point.
- Click **Save** to confirm this access point or **Cancel** to close the page without adding the ignored rogue access point to the list.

Note To modify an existing friendly access point, choose **Configure > Controller Template Launch Pad > Security > Rogue >Ignored Rogue AP**, and click the MAC address of the ignored rogue access point. Make the necessary changes, and click **Save**.

Note If you remove the MAC address from the Ignored AP list, the MAC address is removed from the Rogue AP Ignore-List on the controller.

Configuring 802.11 Templates

This section contains the following topics:

Configuring Load Balancing Templates

To configure load balancing templates, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Load Balancing** or choose **802.11 > Load Balancing** from the left sidebar menu. The Load Balancing page appears.

Step 3 Enter a value between 1 and 20 for the client window size. The page size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

load-balancing page + client associations on AP with lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client page size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

Step 4 Enter a value between 0 and 10 for the max denial count. The denial count sets the maximum number of association denials during load balancing.

Step 5 Click **Save**.

Configuring Band Selection Templates

To configure band selection templates, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Band Select** or choose **802.11 > Band Select** from the left sidebar menu. The Band Select page appears.

Step 3 Enter a value between 1 and 10 for the probe cycle count. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 4 Enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.

Step 5 Enter a value between 10 and 200 seconds for the age out suppression field. Age-out suppression sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 6 Enter a value between 10 and 300 seconds for the age out dual band field. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 7 Enter a value between –20 and –90 dBm for the acceptable client RSSI field. This field sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

Step 8 Click **Save**.

Configuring Preferred Call Templates

This page enables you to create or modify a template for configuring Preferred Call.

To add or modify preferred call templates, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Preferred Call** or choose **802.11 > Preferred Call** from the left sidebar menu. The Preferred Call Controller Templates page appears.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The New Controller Template page appears.

Step 4 Configure the following Preferred Call parameters:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Number Id—Enter a value to identify the preferred number. You can have a maximum of six preferred call numbers. The valid range is from 1 to 6. The default value is 1.
- Preferred Number—Enter the preferred call number.

Step 5 Click **Save**.

Configuring Media Stream for Controller Templates (802.11)

To configure the media stream for a controller template for an 802.11 Radio, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 In the **802.11** group box, click **New** beside Media Stream. The New Controller Template page appears.

Step 3 In the General group box, specify an appropriate name for the template.

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

Step 4 In the Media Stream Configuration group box, specify the following fields:

- Media Stream Name
- Multicast Destination Start IP—Start IP address of the media stream to be multicast.
- Multicast Destination End IP—End IP address of the media stream to be multicast.

Note Start IP and End IP can be IPv4 or IPv6 multicast address from controller Release 7.2.x.

- Maximum Expected Bandwidth—Maximum bandwidth that a media stream can use.

Step 5 In the Resource Reservation Control (RRC) Parameters group box, specify the following fields:

- Average Packet Size—Average packet size that a media stream can use.
- RRC Periodical Update—Resource Reservation Control calculations that are updated periodically; if disabled, RRC calculations are done only once when a client joins a media stream.
- RRC Priority—Priority of RRC with the highest at 1 and the lowest at 8.
- Traffic Profile Violation—Appears if the stream is dropped or put in the best effort queue if the stream violates the QoS video profile.
- Policy—Appears if the media stream is admitted or denied.

Step 6 Click **Save**.

Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 10-2 for more information.

Configuring RF Profiles Templates (802.11)

The RF Profiles page enables you to create or modify RF profiles that get associated to AP Groups.

To configure a RF Profile for a controller template for an 802.11 Radio, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **RF Profiles** or choose either **802.11 > RF Profiles** from the left sidebar menu. The RF Profiles page appears.

Step 3 From the Select a command drop-down list, choose **Add Template**.

Step 4 Click **Go**. The New Controller template page appears.

Step 5 Configure the following information:

- General
  - Template Name—User-defined name for the template.
  - Profile Name—User-defined name for the current profile.
  - Description—Description of the template.
  - Radio Type—The radio type of the access point. This is a drop-down list from which you can choose an RF profile for APs with 802.11a or 802.11b radios.
- TPC (Transmit Power Control)
  - Minimum Power Level Assignment (-10 to 30 dBm)—Indicates the minimum power assigned. Range: -10 to 30 dBm Default: -10 dBm.

  - Maximum Power Level Assignment (-10 to 30 dBm)—Indicates the maximum power assigned. Range: -10 to 30 dBm Default: 30 dBm.
  - Power Threshold v1(-80 to -50 dBm)—Indicates the transmitted power threshold.
  - Power Threshold v2(-80 to -50 dBm)—Indicates the transmitted power threshold.
- Data Rates—Use the Data Rates drop-down lists to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:
  - 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps.
  - 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps

  For each data rate, choose one of these options:
  - Mandatory—Clients must support this data rate to associate to an access point on the controller.
  - Supported—Any associated clients that support this data rate might communicate with the access point using that rate. However, the clients are not required to be able to use this rate to associate.
  - Disabled—The clients specify the data rates used for communication.

Step 6 Click **Save**.

Configuring Radio Templates (802.11a/n)

This section contains the following topics:

Configuring 802.11a/n Parameters Templates

To add or modify radio templates, follow these steps:

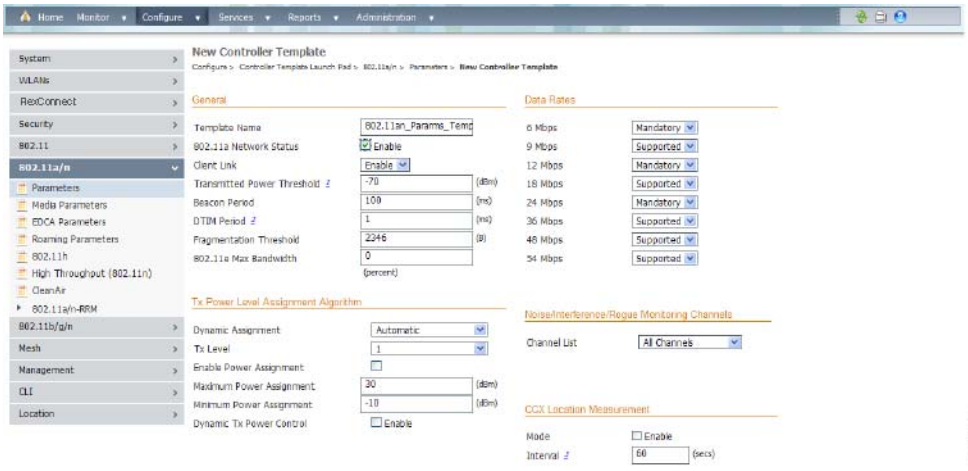
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Parameters** or choose either **802.11a/n > Parameters** from the left sidebar menu. The 802.11a/n Parameters template page appears and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the 802.11 network status and the channel and power mode. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n Parameters template page appears (see Figure 10-46).

Figure 10-46 802.11a/n Parameters Template



Step 4 Select the check box if you want to enable 802.11a/n network status.

Step 5 Use the ClientLink drop-down list to enable Clientlink on all access point 802.11a/n radios that support ClientLink. Otherwise, choose **Disable**.

Step 6 Enter a transmitted power threshold between -50 and -80.

Step 7 Enter the amount of time between beacons in kilomicroseconds. The valid range is from 20 to 1000 milliseconds.

Step 8 Enter the number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count text box is 0. This value is transmitted in the DTIM period field of beacon frames. When client devices receive a beacon that contains a DTIM, they normally wake up to check for pending packets. Longer intervals between DTIMS let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.

Step 9 In the Fragmentation Threshold field, determine the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

Step 10 Enter the percentage for 802.11e maximum bandwidth.

Step 11 Click if you want short preamble enabled.

Step 12 From the Dynamic Assignment drop-down list, choose one of three modes:

- **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
- **On Demand**—Transmit power is updated when the Assign Now button is selected.
- **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.

Step 13 Determine if you want to enable Dynamic Tx Power Control. The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

Step 14 The Assignment Mode drop-down list has three dynamic channel modes:

- **Automatic**—The channel assignment is periodically updated for all access points that permit this operation. This is also the default mode.
- **On Demand**—Channel assignments are updated when desired.
- **OFF**—No dynamic channel assignments occur, and values are set to their global default.

Step 15 Select the **Avoid Foreign AP Interference** check box if you want to enable it. Enable this field to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels. This Radio Resource Management (RRM) field monitors foreign 802.11 interference. Unselect this check box to have RRM ignore this interference.

In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the foreign access points. This increases capacity and reduces variability for the Cisco WLAN Solution.

Step 16 Select the **Avoid Cisco AP Load** check box if you want it enabled. Enable this RRM bandwidth-sensing field to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Unselect this check box to have RRM ignore this value.

In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel reuse. In these circumstances, RRM can assign better reuse patterns to those access points that carry more traffic load.

Step 17 Select the **Avoid non 802.11 Noise** check box if you want to enable it. Enable this RRM noise-monitoring field to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Unselect this check box to have RRM ignore this interference.

In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources. This increases capacity and reduces variability for the Cisco WLAN Solution.

Step 18 The Signal Strength Contribution check box is always enabled (not configurable). RRM constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel reuse. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.

Step 19 The client and controller negotiate data rates between them. If the data rate is set to Mandatory, the client must support it to use the network. If a data rate is set as Supported by the controller, any associated client that also supports that same rate might communicate with the access point using that rate. However, it is not required that a client uses all the rates marked supported to associate. For each rate, a drop-down list of Mandatory or Supported is available. Each data rate can also be set to Disabled to match client settings.

Step 20 From the Channel List drop-down list in the Noise/Interference/Rogue Monitoring Channels section, choose between **all channels**, **country channels**, or **DCA channels** based on the level of monitoring you want. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

Step 21 The location measurement interval of the Cisco Compatible Extension can only be changed when measurement mode is enabled to broadcast radio measurement requests. When enabled, this enhances the location accuracy of clients.

Step 22 Click **Save**.

Configuring Media Parameters Controller Templates (802.11a/n)

This page enables you to create or modify a template for configuring 802.11a/n voice fields such as call admission control and traffic stream metrics.

To add a new template with 802.11a/n voice fields information (such as Call Admission Control and traffic stream metrics) for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **New** beside the template you want to add.

Step 3 Specify an appropriate name for the template.

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

Step 4 On the Voice tab, configure the following fields:

- Admission Control (ACM)—Select the check box to enable admission control.

  For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, call admission control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.

- CAC Method—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.

  Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

- Maximum Bandwidth Allowed—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.

- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.

- Expedited Bandwidth—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.

  You must have an expedited bandwidth IE that is CCXv5 compliant so that a TSPEC request is given higher priority.

- SIP CAC—Select the check box to enable SIP CAC.

  SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.

- SIP Codec—Specify the codec name you want to use on this radio. The available options are **G.711**, **G.729**, and **User Defined**.

- SIP Call Bandwidth—Specify the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.

- SIP Sample Interval—Specify the sample interval in milliseconds that the codec must operate in.

- Max Number of Calls per Radio—Specify the maximum number of calls per Radio.

- Metric Collection—Select the check box to enable metric collection.

  Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Step 5 On the Video tab, configure the following fields:

- Admission Control (ACM)—Select the check box to enable admission control.
- Maximum Bandwidth—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
- Unicast Video Redirect—Select the **Unicast Video Redirect** check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
- Client Minimum Phy Rate—Specify the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
- Multicast Direct Enable—Select the **Multicast Direct Enable** check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
- Maximum Number of Streams per Radio—Specify the maximum number of streams per Radio to be allowed.
- Maximum Number of Streams per Client—Specify the maximum number of streams per Client to be allowed.
- Best Effort QOS Admission—Select the **Best Effort QOS Admission** check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used.

Note If disabled and maximum video bandwidth has been used, then any new client request is rejected.

Step 6 On the General tab, specify the following field:

- Maximum Media Bandwidth (0 to 85%)—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Step 7 Click **Save**.

Once saved, the template appears in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 10-2 for more information.

Configuring EDCA Parameters Through a Controller Template (802.11a/n)

Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

To add or configure 802.11a/n EDCA parameters through a controller template, follow these steps:

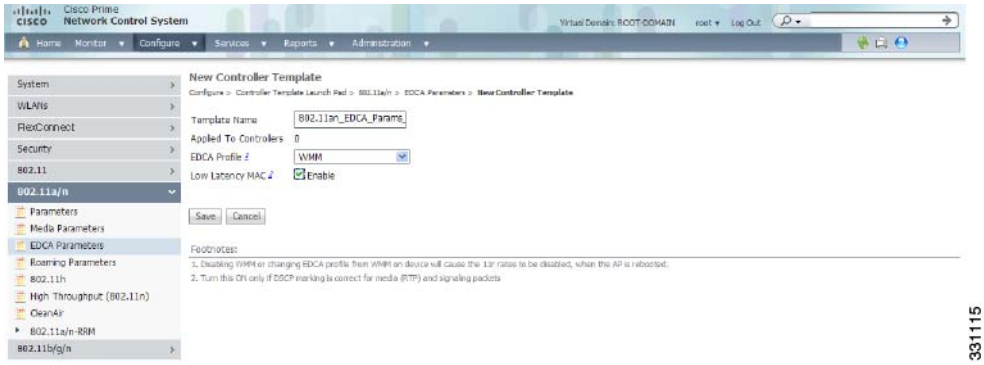
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **EDCA Parameters** or choose **802.11a/n > EDCA Parameters** from the left sidebar menu. The EDCA Parameters template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the EDCP profile and the low latency MAC. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n EDCA Parameters template page appears (see Figure 10-47).

Figure 10-47 802.11a EDCA Parameters



Step 4 Choose one of the following options from the **EDCA Profile** drop-down list:

- **WMM**—Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.
- **Spectralink Voice Priority**—Enables Spectralink voice priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls.
- **Voice Optimized**—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than Spectralink are deployed on your network.
- **Voice & Video Optimized**—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.

Note Video services must be deployed with admission control (ACM). Video services without ACM are not supported.

Note You must shut down radio interface before configuring EDCA Parameters.

Step 5 Select the **Low Latency MAC** check box to enable this feature.

Note Enable low latency MAC only if all clients on the network are WMM compliant.

Configuring a Roaming Parameters Template (802.11a/n)

To add or modify an existing roaming parameter template, follow these steps:

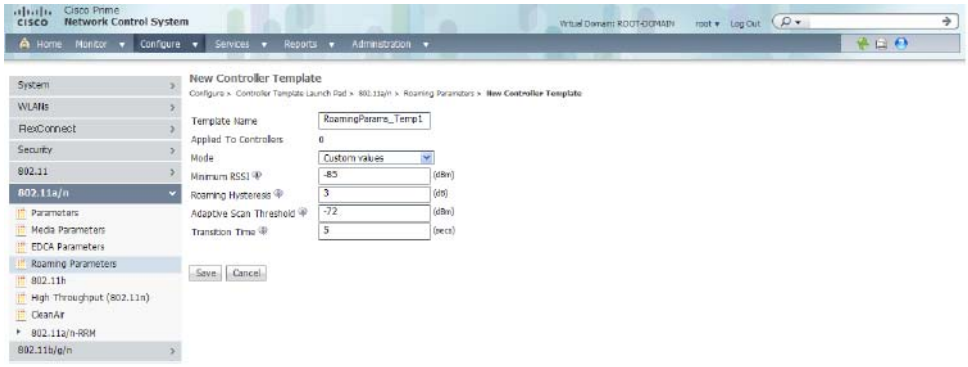
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Roaming Parameters** or choose **802.11a/n > Roaming Parameters** from the left sidebar menu. The Roaming Parameters template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the minimum RSSI, roaming hysteresis, adaptive scan threshold, and transition time. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n Roaming Parameters template page appears (see Figure 10-48).

Figure 10-48 802.11a/n Roaming Parameters Template



Step 4 Use the Mode drop-down list to choose one of the configurable modes: default values and custom values. When the default values option is chosen, the roaming parameters are unavailable with the default values displayed in the text boxes. When the custom values option is selected, the roaming parameters can be edited in the text boxes. To edit the parameters, continue to Step 5.

Step 5 In the Minimum RSSI field, enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point. If the average received signal power of the client dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

Range: -80 to -90 dBm

Default: -85 dBm

Step 6 In the Roaming Hysteresis field, enter a value to indicate how strong the signal strength of a neighboring access point must be for the client to roam to it. This field is intended to reduce the amount of ping ponging between access points if the client is physically located on or near the border between two access points.

Range: 2 to 4 dB

Default: 2 dB

Step 7 In the Adaptive Scan Threshold field, enter the RSSI value from the associated access point of the client, below which the client must be able to roam to a neighboring access point within the specified transition time. This field also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.

Range: -70 to -77 dB

Default: -72 dB

Step 8 In the Transition Time field, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the associated access point of the client is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

Range: 1 to 10 seconds

Default: 5 seconds

Step 9 Click **Save**.

Configuring an 802.11h Template

802.11h informs client devices about channel changes and can limit the transmit power of the client device. Create or modify a template for configuration 802.11h parameters (such as power constraint and channel controller announcement) and applying these settings to multiple controllers.

To add or modify an 802.11h template, follow these steps:

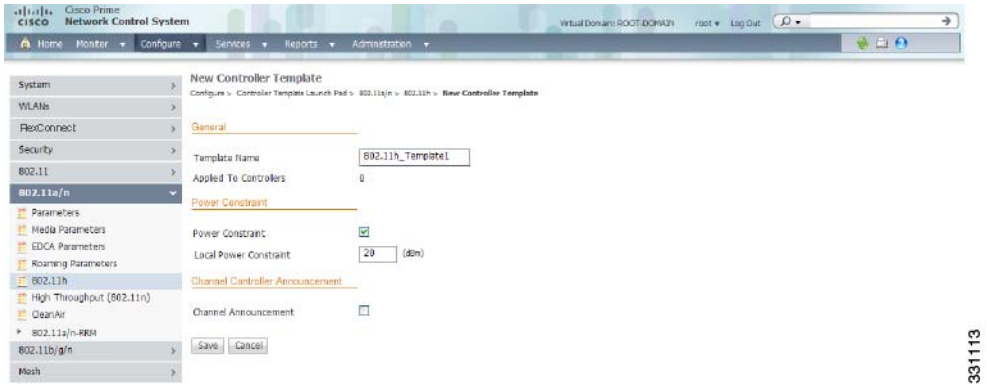
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **802.11h** or choose **802.11a/n > 802.11h** from the left sidebar menu.The 802.11h Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the local power constraint and channel announcement quiet mode. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11h template page appears (see Figure 10-49).

Figure 10-49 802.11h Template



Step 4 Select the **Power Constraint** check box if you want the access point to stop transmission on the current channel.

Step 5 Select the **Channel Announcement** check box to enable channel announcement. Channel announcement is a method in which the access point announces when it is switching to a new channel and the new channel number.

Step 6 Click **Save**.

Configuring a High Throughput Template (802.11a/n)

To add or modify to an 802.11a/n high throughput template, follow these steps:

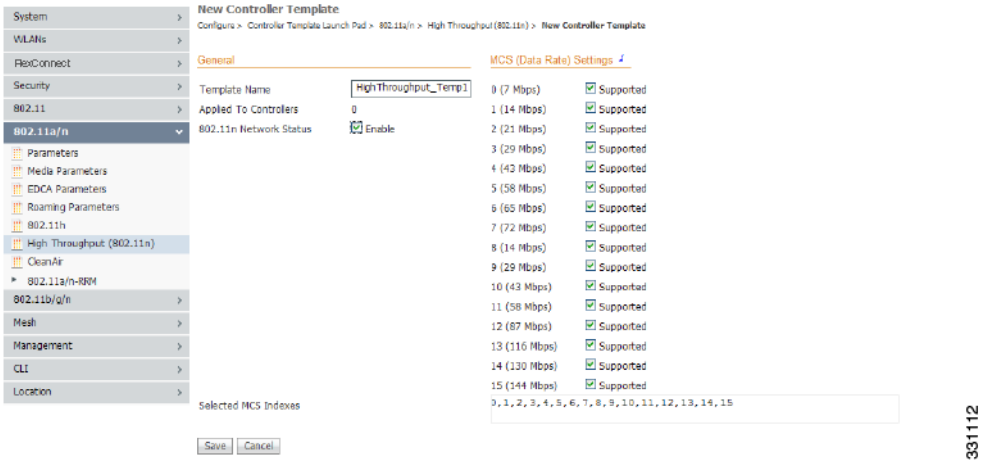
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **High Throughput (802.11n)** or choose **802.11a/n > High Throughput** from the left sidebar menu. The 802.11n Parameters for 2.4 GHz or 802.11n Parameters for 5 GHz Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the 802.11n network status. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n High Throughput template page appears (see Figure 10-50).

Figure 10-50 802.11a/n High Throughput Template



Step 4 Select the **802.11n Network Status Enabled** check box to enable high throughput.

Step 5 In the MCS (Data Rate) Settings column, choose which level of data rate you want supported. Modulation coding schemes (MCS) are similar to 802.11a data rate. As a default, 20 MHz and short guarded interval is used.

Note When you select the Supported check box, the chosen numbers appear in the Selected MCS Indexes page.

Step 6 Click **Save**.

Configuring CleanAir Controller Templates (802.11a/n)

Create or modify a template for configuring CleanAir parameters for the 802.11a/n radio. You can configure the template to enable or disable CleanAir, reporting and alarms for the controllers. You can also configure the type of interfering devices to include for reporting and alarms.

To add a new template with 802.11a/n CleanAir information for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 From the left sidebar menu, choose **802.11a/n > CleanAir**. The 802.11a/n CleanAir Controller Templates page displays all currently saved 802.11a/n CleanAir templates. It also displays and the number of controllers and virtual domains to which each template is applied.

Step 3 From the **Select a command** drop-down list, choose **Add a Template**, and click **Go**.

The **New Controller Template** page appears.

Step 4 Configure the following fields:

- Template Name—Enter the template name.
- CleanAir—Select the check box to enable CleanAir functionality on the 802.11 b/g/n network, or unselect to prevent the controller from detecting spectrum interference.

Note If CleanAir is enabled, the Reporting Configuration and Alarm Configuration group boxes appear.

- Reporting Configuration—Use the fields in this group box to configure the interferer devices you want to include for your reports.

  Report Interferers—Select the **report interferers** check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.

  Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferers to Ignore box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources are ignored.

- Alarm Configuration—This group box enables you to configure triggering of air quality alarms.
  - Air Quality Alarm—Select the **Air Quality Alarm** check box to enable the triggering of air quality alarms, or unselect the box to disable this feature.
  - Air Quality Alarm Threshold—If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold field to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 1.
  - Interferers For Security Alarm—Select the **Interferers For Security Alarm** check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is unselected.
  - Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms box. Use the > and < buttons to move interference sources between these two boxes. By default, all interferer sources for security alarms are ignored.

Step 5 Click **Save**. Once saved, the template appears in the Template List page. In the Template List page, you can apply this template to controllers. See the "Configuring Controller Templates" section on page 10-4 for more information.

Configuring 802.11a/n RRM Templates

This section contains the following topics:

Configuring an RRM Threshold Template (802.11a/n)

To add or make modifications to an 802.11a/n or 802.11b/g/n RRM threshold template, follow these steps:

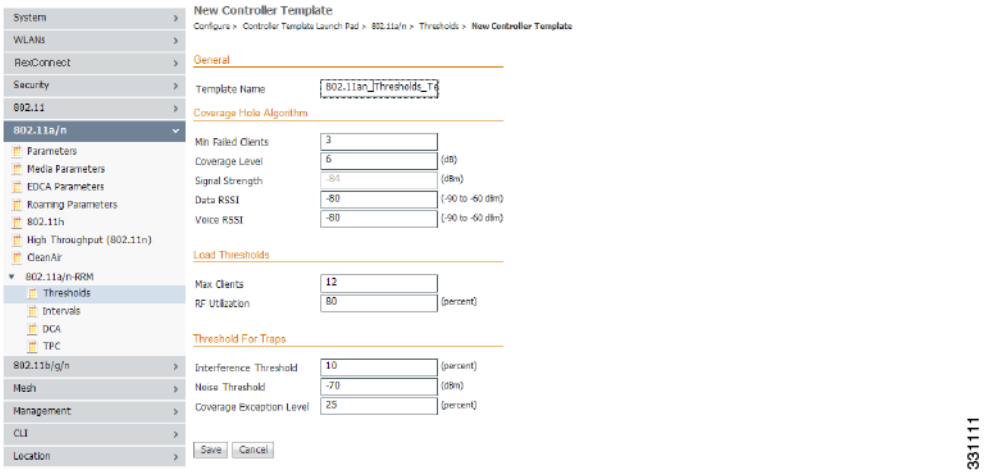
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **RRM Thresholds** or choose **802.11a/n > RRM Thresholds**. The 802.11a/n RRM Thresholds Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the interference and noise threshold, maximum clients, and RF utilization. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n RRM Threshold template page appears (see Figure 10-51).

Figure 10-51 802.11a/n RRM Thresholds Template



Step 4 Enter the minimum number of failed clients currently associated with the controller.

Step 5 Enter the target range of coverage threshold.

Step 6 Enter the Data RSSI (–60 to –90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) for data required for the client to associate to an access point.

Note You must disable the 802.11a/n network before applying these RRM threshold fields.

Step 7 Enter the Voice RSSI (–60 to –90 dBM). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) required for voice for the client to associate to an access point.

Step 8 Enter the maximum number of failed clients that are currently associated with the controller.

Step 9 In the RF Utilization text box, enter the percentage of threshold for 802.11a/n.

Step 10 Enter an interference threshold percentage.

Step 11 Enter a noise threshold between -127 and 0 dBm. When the controller is outside of this threshold, it sends an alarm to the NCS.

Step 12 Enter the coverage exception level percentage. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole is generated.

Step 13 Click **Save**.

Configuring an RRM Interval Template (802.11a/n)

To add or make modifications to an 802.11a/n RRM interval template, follow these steps:

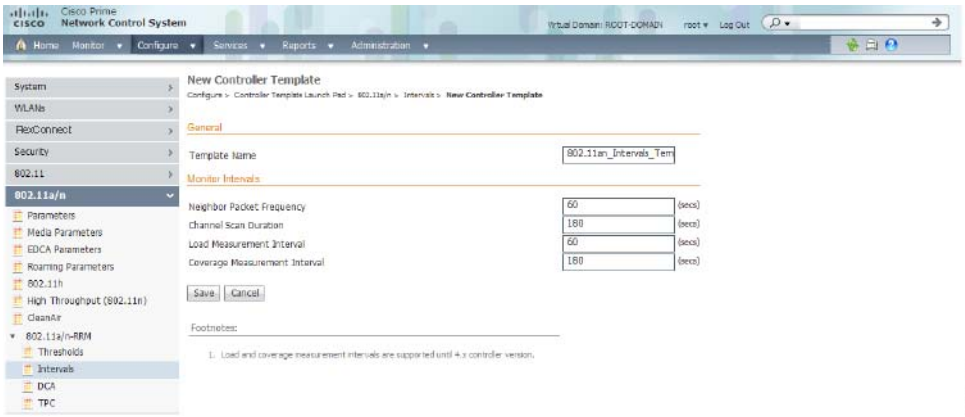
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click RRM Intervals or choose **802.11a/n > RRM Intervals** from the left sidebar menu. The 802.11a/n or 802.11b/g/n RRM Threshold Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the neighbor packet frequency, noise measurement interval, and load measurement interval. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n or 802.11b/g/n RRM Intervals template page appears (see Figure 10-52).

Figure 10-52 802.11a/n RRM Intervals Template



Step 4 In the Neighbor Packet Frequency text box, enter the interval at which you want strength measurements taken for each access point. The default is 300 seconds.

Step 5 Enter the interval at which you want noise and interference measurements taken for each access point. The default is 300 seconds.

Step 6 Enter the interval at which you want load measurements taken for each access point. The default is 300 seconds.

Step 7 At the Coverage Measurement Interval field, enter at which interval you want coverage measurements taken for each access point. The default is 300 seconds.

Step 8 Click **Save**.

Configuring an RRM Dynamic Channel Allocation Template (802.11a/n)

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.

Note Choosing a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments.

To configure 802.11 a/n RRM DCA template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **DCA** or choose **802.11a/n > DCA**. The 802.11a/n DCS Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n TPC template page appears.

Step 4 Configure the following fields:

- Template Name—Enter the template name.
- **Assignment Mode**—From the Dynamic Assignment drop-down list, choose one of three modes:
  - **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
  - **On Demand**—Transmit power is updated when you click **Assign Now**.
  - **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.
- Select the **Avoid Foreign AP Interference** check box to enable it. Enable this check box to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels. This foreign 802.11 interference. Unselect this check box to have RRM ignore this interference.

  In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the foreign access points. This increases capacity and reduces variability for the Cisco WLAN Solution.
- Select the **Avoid Cisco AP Load** check box if you want it enabled. Enable this bandwidth-sensing field to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Unselect this check box to have RRM ignore this value.

  In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel reuse. In these circumstances, RRM can assign better reuse patterns to those access points that carry more traffic load.

- Select the **Avoid non 802.11 Noise** check box if you want to enable it. Enable this noise-monitoring field to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Unselect this check box to have RRM ignore this interference.

  In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources. This increases capacity and reduces variability for the Cisco WLAN Solution.

- The Signal Strength Contribution check box is always enabled (not configurable). This constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel reuse. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.

- Enable or disable event-driven Radio Resource Management (RRM) using the following fields. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference.
  - Event Driven RRM—Enable or Disable spectrum event-driven RRM. By default, Event Driven RRM is enabled.
  - Sensitivity Threshold—If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Step 5 Click **Save**.

Configuring an RRM Transmit Power Control Template (802.11a/n)

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of the access points according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

To configure 802.11a/n RRM TPC template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **TPC** or choose **802.11a/n > TPC**. The 802.11a/n TPC Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n TPC template page appears.

Step 4 Configure the following fields:

- Template Name—Enter the template name in the text box.
- TPC Version—Choose TPCv1 or TPCv2.

Note The TPCv2 option is applicable only for those controllers running Release 7.2.x or later.

- Dynamic Assignment—From the Dynamic Assignment drop-down list, choose one of three modes:
  - **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
  - **On Demand**—Transmit power is updated when you click **Assign Now**.
  - **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.
- Maximum Power Assignment—Indicates the maximum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Minimum Power Assignment—Indicates the minimum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Dynamic Tx Power Control—Determine if you want to enable Dynamic Tx Power Control.
- Transmitted Power Threshold—Enter a transmitted power threshold between -50 and -80.
- Control Interval—In seconds (read-only).

Step 5 Click **Save**.

Configuring Radio Templates (802.11b/g/n)

This section contains the following topics:

- Configuring 802.11b/g/n RRM Templates, page 10-117

Configuring 802.11b/g/n Parameters Templates

Create or modify a template for configuring 802.11b/g/n parameters (such as power and channel status, data rates, channel list, and CCX location measurement) and/or applying these settings to controller(s).

To add a new template with 802.11b/g/n parameters information for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **New** beside the template you want to add.

Step 3 Configure the following General parameters:

- Policy Name—Security policy in force.
- 802.11b/g Network Status
- Beam Forming—Choose **Enable** or **Disable** from the drop-down list.

Note Beam forming refers to a general signal processing technique used to control the directionality of the reception or transmission of a signal.

- Transmitted Power Threshold—The valid range is from -50 to -80.
- Beacon Period—The rate at which the SSID is broadcast by the access point (the amount of time between beacons). The valid range is from 100 to 600 milliseconds.
- DTIM Period—The number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count field is 0. This value is transmitted in the DTIM period field of beacon frames.

  When client devices receive a beacon that contains a DTIM, they normally “wake up” to check for pending packets. Longer intervals between DTIMs let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.

Note DTIM period is not applicable in controller Release 5.0.0.0 and later.

- Fragmentation Threshold—Determine the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference. The default value is 2346.
- 802.11e Max Bandwidth—Percentage for 802.11e max bandwidth. The default value is 100.

Step 4 Configure the following 802.11b/g Power Status parameters:

- Dynamic Assignment—From the Dynamic Assignment drop-down list, choose any one of the following dynamic transmit power assignment modes.
  - **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
  - **On Demand**—Transmit power is updated when you click **Assign Now**.
  - **Disabled**—No dynamic transmit power assignments occur and values are set to their global default. The default is Automatic.

Note The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

- Dynamic Tx Power Control—Select this check box to enable DTPC support. If this option is enabled, the transmit power level of the radio is advertised in the beacons and the probe responses.

Step 5 Configure the following 802.11b/g Channel Status parameters:

- Assignment Mode—From the Assignment Mode drop-down list, choose any one of the following dynamic channel assignment modes.
  - **Automatic**—The channel assignment is periodically updated for all access points that permit this operation.
  - **On Demand**—Channel assignments are updated when desired.
  - **Disabled**—No dynamic channel assignments occur and values are set to their global default.

  Note The default is Automatic.

- Avoid Foreign AP Interference—Enable this Radio Resource Management (RRM) foreign 802.11 interference-monitoring parameter to have Radio Resource Management consider interference from foreign (non-Cisco access points outside the RF/mobility domain) access points when assigning channels to Cisco access points.

  Disable this field to have Radio Resource Management ignore this interference.

  Note In certain circumstances with significant interference energy (dB) and load (utilization) from Foreign access points, Radio Resource Management might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in Cisco access points close to the Foreign access points to increase capacity and reduce variability for the Cisco WLAN Solution.

- Avoid Cisco AP Load—Enable this Radio Resource Management (RRM) bandwidth-sensing parameter to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points.

  Disable this field to have Radio Resource Management ignore this value.

  Note In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel re-use. In these circumstances, Radio Resource Management can assign better re-use patterns to those APs that carry more traffic load.

- Avoid non 802.11 Noise—Enable this Radio Resource Management (RRM) noise-monitoring field to have access points avoid channels that have interference from non-Access Point sources, such as microwave ovens or Bluetooth devices.

  Disable this field to have Radio Resource Management ignore this interference.

Note In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, Radio Resource Management might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources to increase capacity and reduce variability for the Cisco WLAN Solution.

- Signal Strength Contribution—This check box is always enabled (not configurable). Radio Resource Management (RRM) constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel reuse. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.

Step 6 Configure the Data Rate parameters.

The data rates set are negotiated between the client and the controller. If the data rate is set to Mandatory, the client must support it to use the network. If a data rate is set as Supported by the controller, any associated client that also supports that same rate might communicate with the access point using that rate. But it is not required that a client be able to use all the rates marked Supported to associate 6, 9, 12, 18, 24, 36, 48, 54 Mbps. For each rate, a drop-down list selection of Mandatory or Supported is available. Each data rate can also be set to Disabled to match Client settings.

Step 7 Configure the Noise/Interference/Rogue Monitoring Channels parameters.

Choose between all channels, country channels, or DCA channels based on the level of monitoring you want. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation among a set of managed devices connected to the controller.

Step 8 Configure the CCX Location Measurement parameters:

- Mode—Enable or disable the broadcast radio measurement request. When enabled, this enhances the location accuracy of clients.
- Interval—Interval in seconds between requests.

Note Cisco Compatible Extension location measurement interval can be changed only when measurement mode is enabled.

Step 9 Click **Save**. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 10-2 for more information.

Configuring Media Parameters Controller Templates (802.11b/g/n)

Create or modify a template for configuring 802.11b/g/n voice parameters such as Call Admission Control and traffic stream metrics.

To add a new template with 802.11b/g/n voice parameters information (such as Call Admission Control and traffic stream metrics) for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **New** beside the template you want to add.

Step 3 Specify an appropriate name for the template.

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

Step 4 On the Voice tab, configure the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.

  For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, Call Admission Control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.

- CAC Method—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.

  Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

- Maximum Bandwidth Allowed—Enter the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.

- Reserved Roaming Bandwidth—Enter the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.

- Expedited Bandwidth—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.

  You must have an expedited bandwidth IE that is CCXv5 compliant so that a TSPEC request is given higher priority.

- SIP CAC—Select the check box to enable SIP CAC.

  SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.

- SIP Codec—Choose the codec name you want to use on this radio from the SIP Codec drop-don list. The available options are G.711, G.729, and User Defined.

- SIP Call Bandwidth—Enter the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.

- SIP Sample Interval—Enter the sample interval in milliseconds that the codec must operate in.

- Max Number of Calls per Radio—Enter the maximum number of calls per radio.

- Metric Collection—Select the check box to enable metric collection.

  Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Step 5 On the Video tab, configure the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.

- Maximum Bandwidth—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.

- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
- Unicast Video Redirect—Select the **Unicast Video Redirect** check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
- Client Minimum Phy Rate—Choose the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
- Multicast Direct Enable—Select the **Multicast Direct Enable** check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
- Maximum Number of Streams per Radio—Specify the maximum number of streams per Radio to be allowed.
- Maximum Number of Streams per Client—Specify the maximum number of streams per Client to be allowed.
- Best Effort QOS Admission—Select the **Best Effort QOS Admission** check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used.

Note If disabled and maximum video bandwidth has been used, then any new client request is rejected.

Step 6 On the General tab, specify the following field:

- Maximum Media Bandwidth (0 to 85%)—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Step 7 Click **Save**.

Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 10-2 for more information.

Configuring EDCA Parameters Controller Templates (802.11b/g/n)

Create or modify a template for configuring 802.11b/g/n EDCA parameters. EDCA parameters designate pre-configured profiles at the MAC layer for voice and video.

To add a new template with 802.11b/g/n EDCA parameters information for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **New** beside the template you want to add.

Step 3 Configure the following parameters:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- EDCA Profile—Profiles include Wi-Fi Multimedia (WMM), Spectralink Voice Priority (SVP), Voice Optimized, and Voice & Video Optimized. WMM is the default EDCA profile.

Note You must shut down radio interface before configuring EDCA Parameters.

- Streaming MAC—Only enable streaming MAC if all clients on the network are WMM compliant.

Step 4 Click **Save**. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 10-2 for more information.

Configuring Roaming Parameters Controller Templates (802.11b/g/n)

Create or modify a template for configuring roaming parameters for 802.11b/g/n radios.

To add a new template with 802.11b/g/n Roaming parameters information for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **New** beside the template you want to add.

Step 3 Configure the following parameters:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Mode—Choose **Default Values** or **Custom Values** from the drop-down list.
  - Default Values—The roaming parameters are unavailable and the default values are displayed.
  - Custom Values—The following roaming parameters can be edited.
- Minimum RSSI—Enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point.

  If the client average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.
  - Range: -80 to -90 dBm
  - Default: -85 dBm
- Roaming Hysteresis—Enter a value to indicate how strong the signal strength of a neighboring access point must be in order for the client to roam to it. This field is intended to reduce the amount of "ping ponging" between access points if the client is physically located on or near the border between two access points.
  - Range: 2 to 4 dB
  - Default: 2 dB
- Adaptive Scan Threshold—Enter the RSSI value, from a client associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time.

This field also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.

  - Range: -70 to -77 dB
  - Default: -72 dB

- Transition Time—Enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client associated access point is below the scan threshold.
  - Range: 1 to 10 seconds
  - Default: 5 seconds

Note The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

Step 4 Click **Save**. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 10-2 for more information.

Configuring High Throughput (802.11n) Controller Templates (802.11b/g/n)

Create or modify a template for configuring high-throughput parameters such as MCS (data rate) settings and indexes and for applying these 802.11n settings to multiple controllers.

To add a new template with High Throughput (802.11n) information for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **New** beside the template you want to add.

Step 3 Configure the following fields:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- 802.11n Network Status—Select the check box to enable high throughput.
- MCS (Data Rate) Settings—Choose which level of data rate you want supported. MCS is modulation coding schemes which are similar to 802.11a data rate.

Note As a default, 20 MHz and short guarded interval are used.

Note When you select the Supported check box, the chosen numbers appear in the Selected MCS Indexes page.

Step 4 Click **Save**. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 10-2 for more information.

Configuring CleanAir Controller Templates (802.11 b/g/n)

Create or modify a template for configuring CleanAir parameters for the 802.11 b/g/n radio. You can configure the template to enable or disable CleanAir, reporting and alarms for the controllers. You can also configure the type of interfering devices to include for reporting and alarms.

To add a new template with 802.11b/g/n CleanAir information for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 From the left sidebar menu, choose **802.11b/g/n > CleanAir**. The 802.11b/g/n CleanAir Controller Templates page displays all currently saved 802.11b/g/n CleanAir templates. It also displays and the number of controllers and virtual domains to which each template is applied.

Step 3 From the Select a command drop-down list, choose **Add a Template**, and click **Go**.

The **New Controller Template** page appears.

Step 4 Configure the following fields:

- Template Name—Enter the template name in the text box.
- CleanAir—Select the check box to enable CleanAir functionality on the 802.11 b/g/n network, or unselect to prevent the controller from detecting spectrum interference. The default value is selected.

Note If CleanAir is enabled, the Reporting Configuration and Alarm Configuration group boxes appear.

- Reporting Configuration—Use the parameters in this group box to configure the interferer devices you want to include for your reports.
  - Report Interferers—Select the **report interferers** check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.
  - Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferers to Ignore box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources are ignored.
- Alarm Configuration—This group box enables you to configure triggering of air quality alarms.
  - Air Quality Alarm—Select the **Air Quality Alarm** check box to enable the triggering of air quality alarms, or unselect the box to disable this feature.

- Air Quality Alarm Threshold—If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 1.
- Interferers For Security Alarm—Select the **Interferers For Security** Alarm check box to trigger interferer alarms when the controller detects specified device types, or unselected it to disable this feature. The default value is unselected.
- Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms box. Use the **>** and **<** buttons to move interference sources between these two boxes. By default, all interferer sources for security alarms are ignored.

Step 5 Click **Save**. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the "Adding Controller Templates" section on page 10-2 for more information.

Configuring 802.11b/g/n RRM Templates

This section contains the following topics:

Configuring RRM Thresholds Controller Templates (802.11b/g/n)

Create or modify a template for setting various RRM thresholds such as load, interference, noise, and coverage.

To add a new template with 802.11b/g/n RRM thresholds information for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **New** beside the template you want to add.

Step 3 Add or modify the following template name.

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

Step 4 Configure the following Coverage Hole Algorithm parameters:

- Min. Failed Clients (#)—Enter the minimum number of failed clients currently associated with the controller.
- Coverage Level—Enter the target range of coverage threshold (dB).

- Signal Strength—When the Coverage Level field is adjusted, the value of the Signal Strength (dBm) automatically reflects this change. The Signal Strength field provides information regarding what the signal strength is when adjusting the coverage level.
- Data RSSI—Enter the Data RSSI (-60 to -90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) for data required for the client to associate to an access point.
- Voice RSSI—Enter the Voice RSSI (-60 to -90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) required for voice for the client to associate to an access point.

Step 5 Configure the following Load Thresholds parameters:

- Max. Clients—Enter the maximum number of clients able to be associated with the controller.
- RF Utilization—Enter the percentage of threshold for this radio type.

Step 6 Configure the following Threshold for Traps parameters:

- Interference Threshold—Enter an interference threshold between 0 and 100 percent.
- Noise Threshold—Enter a noise threshold between -127 and 0 dBm. When outside of this threshold, the controller sends an alarm to the NCS.
- Coverage Exception Level—Enter the coverage exception level percentage. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole is generated.

Step 7 Click **Save**. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 10-2 for more information.

Configuring RRM Intervals Controller Templates (802.11b/g/n)

Create or modify a template for configuring RRM intervals for 802.11b/g/n radios.

To add a new template with 802.11b/g/n RRM intervals information for a controller, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **New** beside the template you want to add.

Step 3 Configure the following parameters:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Neighbor Packet Frequency—Enter at which interval you want strength measurements taken for each access point. The default is 300 seconds.
- Noise Measurement Interval—Enter at which interval you want noise and interference measurements taken for each access point. The default is 180 seconds.
- Load Measurement Interval—Enter at which interval you want load measurements taken for each access point. The default is 300 seconds.

- Channel Scan Duration—Enter at which interval you want coverage measurements taken for each access point. The default is 300 seconds.

Step 4 Click **Save**. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 10-2 for more information.

Configuring an RRM Dynamic Channel Allocation Template (802.11b/g/n)

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.

Note Choosing a larger bandwidth reduces the non-overlapping channels, which could potentially reduce the overall network throughput for certain deployments.

To configure 802.11b/g/n RRM DCA template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **DCA** or choose **802.11b/g/n > DCA**. The 802.11b/g/n DCS Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11b/g/n TPC template page appears.

Step 4 Configure the following parameters:

- Template Name—Enter the template name.
- Assignment Mode—From the Dynamic Assignment drop-down list, choose one of three modes:
  - **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
  - **On Demand**—Transmit power is updated when you click **Assign Now**.
  - **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.
- Select the **Avoid Foreign AP Interference** check box to enable it. Enable this field to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels. This foreign 802.11 interference. Unselect this check box to have RRM ignore this interference.

In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the foreign access points. This increases capacity and reduces variability for the Cisco WLAN Solution.

- Select the **Avoid Cisco AP Load** check box if you want it enabled. Enable this bandwidth-sensing field to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Unselect this check box to have RRM ignore this value.

  In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel reuse. In these circumstances, RRM can assign better re-use patterns to those access points that carry more traffic load.

- Select the **Avoid non 802.11 Noise** check box if you want to enable it. Enable this noise-monitoring field to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Unselect this check box to have RRM ignore this interference.

  In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources. This increases capacity and reduces variability for the Cisco WLAN Solution.

- The **Signal Strength Contribution** check box is always enabled (not configurable). constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel re-use. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.

- Enable or disable event-driven Radio Resource Management (RRM) using the following parameters. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference.

  – Event Driven RRM—Enable or Disable spectrum event-driven RRM. By default, Event Driven RRM is enabled.

  – Sensitivity Threshold—If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Step 5 Click **Save**.

Configuring an RRM Transmit Power Control Template (802.11b/g/n)

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of an access point according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points.

This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

To configure 802.11b/g/n RRM TPC template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **TPC** or choose **802.11b/g/n > TPC**. The 802.11b/g/n TPC Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11b/g/n TPC template page appears.

Step 4 Configure the following parameters:

- Template Name—Enter the template name in the text box.
- TPC Version—Choose TPCv1 or TPCv2 from the drop-down list.

Note The TPCv2 option is applicable only for those controller Release 7.2.x or later.

- Dynamic Assignment—From the Dynamic Assignment drop-down list, choose one of three modes:
  - **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
  - **On Demand**—Transmit power is updated when you click **Assign Now**.
  - **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.
- Maximum Power Assignment—Indicates the maximum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Minimum Power Assignment—Indicates the minimum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Dynamic Tx Power Control—Determine if you want to enable Dynamic Tx Power Control.
- Transmitted Power Threshold—Enter a transmitted power threshold between -50 and -80.
- Control Interval—In seconds (read-only).

Step 5 Click **Save**.

Configuring Mesh Templates

Configuring Mesh Setting Templates

You can configure an access point to establish a connection with the controller.

To add or modify a mesh template, follow these steps:

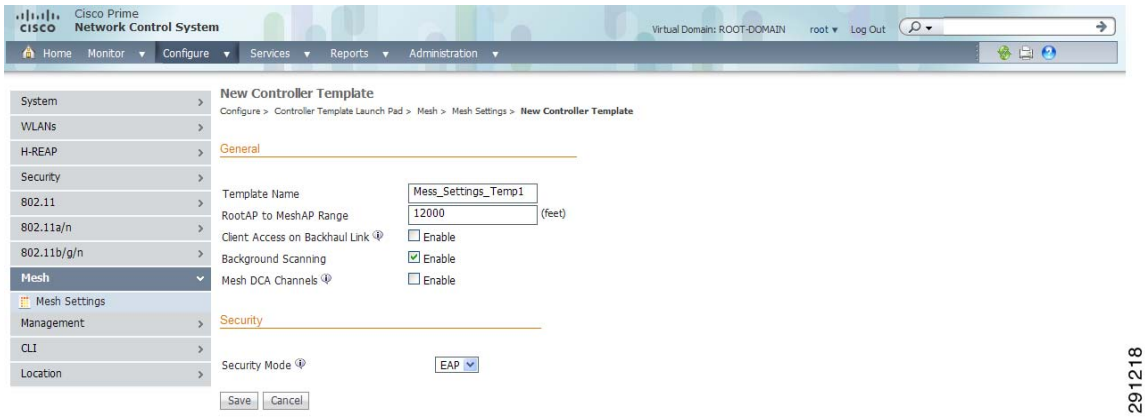
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Mesh Configuration** or choose **Mesh > Mesh Configuration** from the left sidebar menu. The Mesh Configuration Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the rootAP to MeshAP range, the client access on backhaul link, and security mode. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Mesh Configuration template page appears (see Figure 10-53).

Figure 10-53 Mesh Configuration Template



Step 4 The Root AP to Mesh AP Range is 12,000 feet by default. Enter the optimum distance (in feet) that should exist between the root access point and the mesh access point. This global field applies to all access points when they join the controller and all existing access points in the network.

Step 5 The **Client Access on Backhaul Link** check box is not selected by default. When this option is enabled, mesh access points can associate with 802.11a/n wireless clients over the 802.11a/n backhaul. This client association is in addition to the existing communication on the 802.11a/n backhaul between the root and mesh access points.

Note This feature applies only to access points with two radios.

Step 6 The **Mesh DCA Channels** check box is not selected by default. Select this option to enable backhaul channel deselection on the Controller using the DCA channel list configured in the Controller. Any change to the channels in the Controller DCA list is pushed to the associated access points. This feature applies only to the 1524SB mesh access points. For more information on this feature, see the *Controller Configuration Guide.*

Step 7 Select the **Background Scanning** check box to enable background scanning or unselect it to disable the feature. The default value is disabled. Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents. See the "Background Scanning on 1510s in Mesh Networks" section on page 8-54 for further information.

Step 8 From the Security Mode drop-down list, choose **EAP** (Extensible Authentication Protocol) or **PSK** (Pre-Shared Key).

Step 9 Click **Save**.

Configuring Management Templates

This section contains the following topics:

Configuring Trap Receiver Templates

If you have monitoring devices on your network that receive SNMP traps, you might want to add a trap receiver template.

To add or modify a trap receiver template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Trap Receivers** or choose **Management > Trap Receivers** from the left sidebar menu.

Step 3 The Management > Trap Receiver page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the IP address and admin status. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 4 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Trap Receivers template page appears (see Figure 10-54).

Figure 10-54 Trap Receivers Template

Step 5 Enter the IP address of the server in the text box.

Step 6 Select the **Admin Status** check box to enable the administrator status if you want SNMP traps to be sent to the receiver.

Step 7 Click **Save**.

Configuring Trap Control Templates

To add or modify a trap control template, follow these steps:

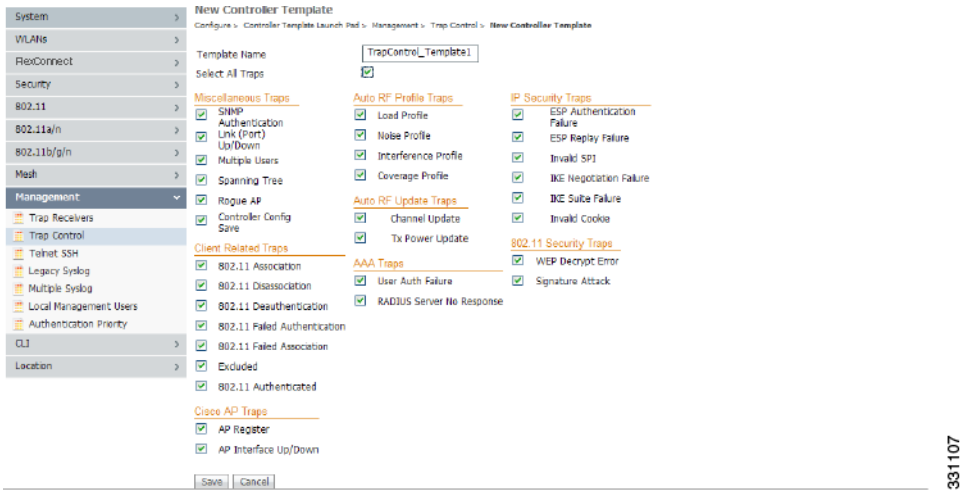
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Trap Control** or choose **Management > Trap Control** from the left sidebar menu. The Management > Trap Control page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the link port up or down and rogue AP. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Trap Control template page appears (see Figure 10-55).

Figure 10-55 Trap Control Template



Step 4 Select the appropriate check box to enable any of the following miscellaneous traps:

- SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated. When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.
- Link (Port) Up/Down—Link changes states from up or down.
- Multiple Users—Two users log in with the same login ID.
- Spanning Tree—Spanning Tree traps. See the STP specification for descriptions of individual parameters.
- Rogue AP—Whenever a rogue access point is detected or when a rogue access point was detected earlier and no longer exists, this trap is sent with its MAC address.
- Controller Config Save—Notification sent when the configuration is modified.

Step 5 Select the appropriate check box to enable any of the following client-related traps:

- 802.11 Association—A trap is sent when a client is associated to a WLAN. This trap does not guarantee that the client is authenticated.
- 802.11 Disassociation—The disassociate notification is sent when the client sends a disassociation frame.
- 802.11 Deauthentication—The deauthenticate notification is sent when the client sends a deauthentication frame.
- 802.11 Failed Authentication—The authenticate failure notification is sent when the client sends an authentication frame with a status code other than successful.
- 802.11 Failed Association—The associate failure notification is sent when the client sends an association frame with a status code other than successful.
- Excluded—The associate failure notification is sent when a client is excluded.

Step 6 Select the appropriate check box to enable any of the following access point traps:

- AP Register—Notification sent when an access point associates or disassociates with the controller.
- AP Interface Up/Down—Notification sent when access point interface (802.11a/n or 802.11b/g/n) status goes up or down.

Step 7 Select the appropriate check box to enable any of the following auto RF profile traps:

- Load Profile—Notification sent when Load Profile state changes between PASS and FAIL.
- Noise Profile—Notification sent when Noise Profile state changes between PASS and FAIL.
- Interference Profile—Notification sent when Interference Profile state changes between PASS and FAIL.
- Coverage Profile—Notification sent when Coverage Profile state changes between PASS and FAIL.

Step 8 Select the appropriate check box to enable any of the following auto RF update traps:

- Channel Update—Notification sent when the dynamic channel algorithm of an access point is updated.
- Tx Power Update—Notification sent when the dynamic transmit power algorithm of an access point is updated.

Step 9 Select the appropriate check box to enable any of the following AAA traps:

- User Auth Failure—This trap is to inform you that a client RADIUS authentication failure has occurred.
- RADIUS Server No Response—This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.

Step 10 Select the appropriate check box to enable the following IP security traps:

- ESP Authentication Failure
- ESP Replay Failure
- Invalid SPI
- IKE Negotiation Failure
- IKE Suite Failure
- Invalid Cookie

Step 11 Select the appropriate check box to enable the following 802.11 security trap:

- WEP Decrypt Error—Notification sent when the controller detects a WEP decrypting error.
- Signature Attack

Step 12 Click **Save**.

Configuring Telnet SSH Templates

To add or modify a Telnet SSH configuration template, follow these steps:

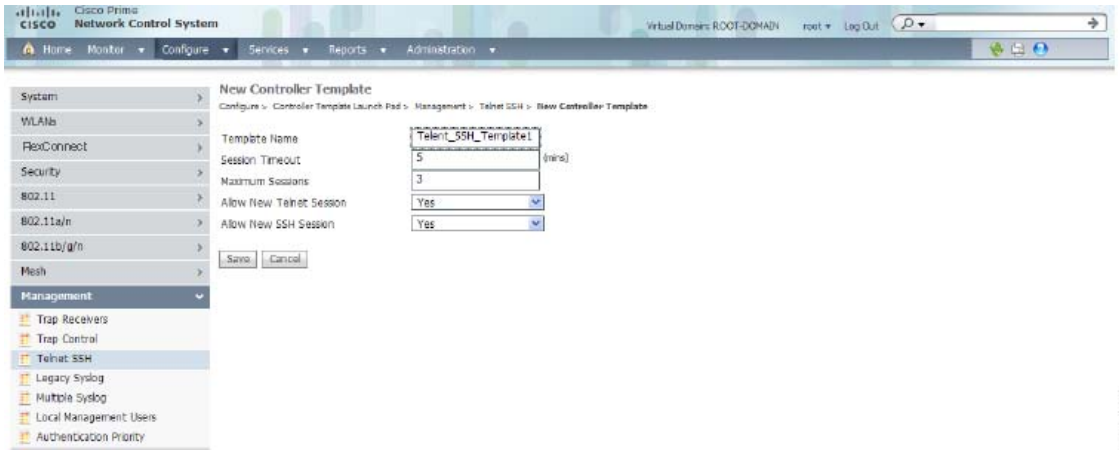
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Telnet SSH** or choose **Management > Telnet SSH** from the left sidebar menu. The Management > Telnet SSH Configuration page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the session timeout, maximum sessions, and whether Telnet or SSH sessions are allowed. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Telnet SSH template page appears (see Figure 10-56).

Figure 10-56 Telnet SSH Template



Step 4 Enter the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. The valid range is 0 to 160, and the default is 5.

Step 5 At the Maximum Sessions field, enter the number of simultaneous Telnet sessions allowed. The valid range is 0 to 5, and the default is 5. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the service port.

Step 6 Use the Allow New Telnet Session drop-down list to determine if you want new Telnet sessions allowed on the DS port. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the service port. The default is no.

Step 7 Use the Allow New SSH Session drop-down list to determine if you want Secure Shell Telnet sessions allowed. The default is yes.

Step 8 Click **Save**.

Configuring Legacy Syslog Templates

To add or modify a legacy syslog configuration template, follow these steps:

Note Legacy Syslog applies to controllers Release 5.0.6.0 and earlier.

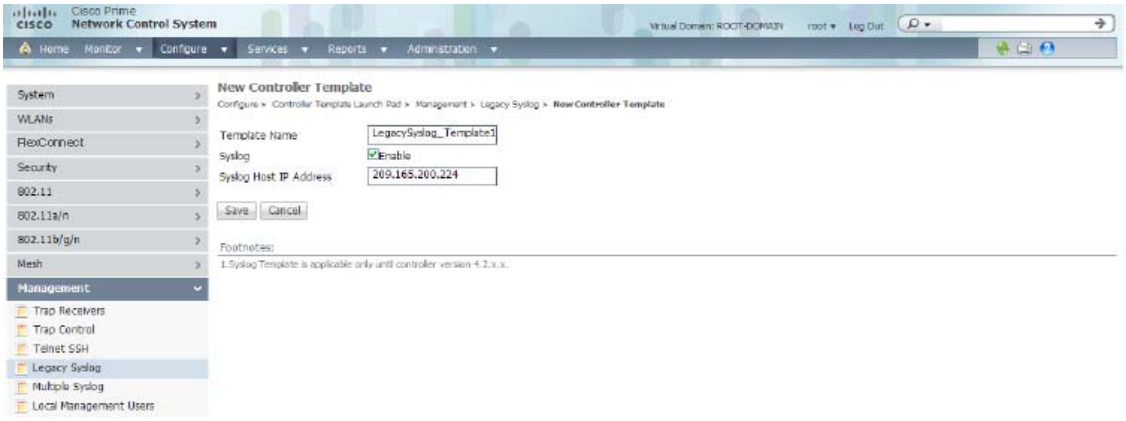
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Legacy Syslog** or choose **Management > Legacy Syslog** from the left sidebar menu. The Management > Legacy Syslog page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Legacy Syslog template page appears (see Figure 10-57).

Figure 10-57 Legacy Syslog Template



Step 4 Enter a template name. The number of controllers to which this template is applied is displayed.

Step 5 Select the **Syslog** check box to enable syslog. When you do, a Syslog Host IP Address text box appears.

Step 6 Click **Save**.

Configuring Multiple Syslog Templates

To add or modify a multiple syslog configuration template, follow these steps:

Note You can enter up to three syslog server templates.

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Multiple Syslog** or choose **Management > Multiple Syslog** from the left sidebar menu. The Management > Multiple Syslog page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the syslog server address. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Multiple Syslog template page appears (see Figure 10-58).

Figure 10-58 Multiple Syslog Template Page

Step 4 Enter a template name and a syslog server IP address in the text boxes.

Step 5 Click **Save**.

Configuring Local Management User Templates

To add or modify a local management user template, follow these steps:

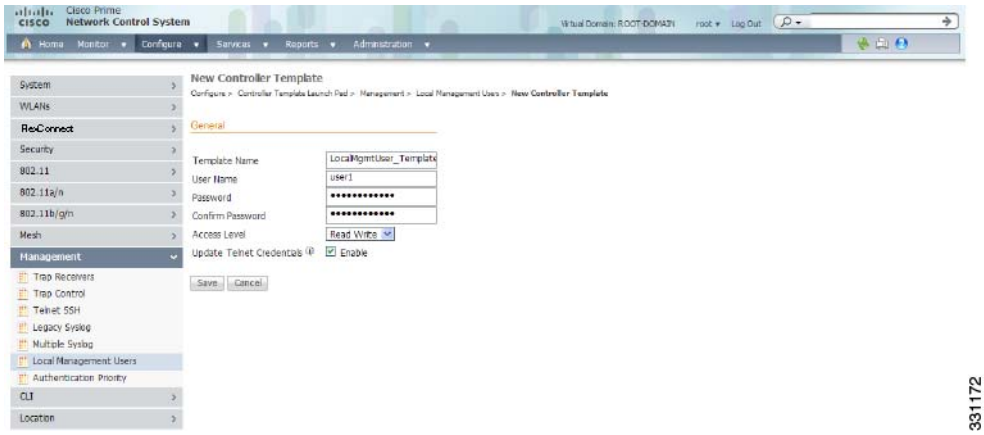
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Local Management Users** or choose **Management > Local Management Users** from the left sidebar menu. The Management > Local Management Users Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the username and access level. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Local Management Users template page appears (see Figure 10-59).

Figure 10-59 Local Management Users Template



Step 4 Enter a template name

Step 5 Enter a template username.

Step 6 Enter a password for this local management user template.

Step 7 Reenter the password.

Step 8 Use the Access Level drop-down list to choose either **Read Only** or **Read Write**.

Step 9 Select the **Update Telnet Credentials** check box to update the user credentials in the NCS for Telnet/SSH access.

Note If the template is applied successfully and the Update Telnet Credentials option is enabled, the applied management user credentials are used in the NCS for Telnet/SSH credentials to that applied controller.

Step 10 Click **Save**.

Configuring User Authentication Priority Templates

Management user authentication priority templates control the order in which authentication servers are used to authenticate the management users of a controller.

To add a user authentication priority template or make modifications to an existing template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Authentication Priority** or choose **Management > Authentication Priority** from the left sidebar menu. The Management > Local Management Users Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the authentication priority list. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Local Management Users template page appears (see Figure 10-60).

Figure 10-60 User Authentication Priority Template

Step 4 Enter a template name.

Step 5 The local server is tried first. Choose either **RADIUS** or **TACACS+** from the drop-down list to try if local authentication fails.

Step 6 Click **Save**.

Configuring CLI Templates

Applying a Set of CLI Commands

You can create templates containing a set of CLI commands and apply them to one or more controllers from the NCS. These templates are meant for provisioning features in multiple controllers for which there is no SNMP support or custom NCS user interface. The template contents are simply a command array of strings. No support for substitution variables, conditionals, and the like exist.

The CLI sessions to the device are established based on user preferences. The default protocol is SSH. See the "Configuring Protocols for CLI Sessions" section on page 15-58 for information on setting protocol user preferences.

To add or modify a CLI template, follow these steps:

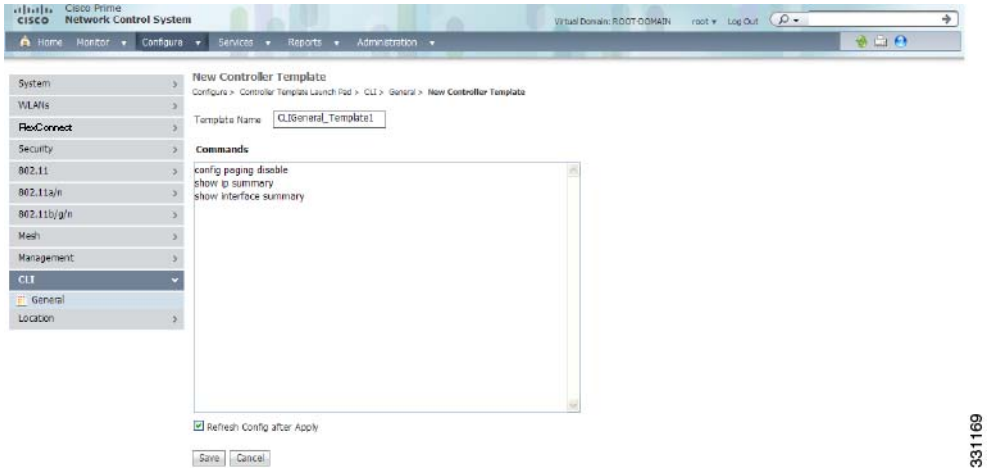
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **CLI > General** or choose **CLI > General** from the left sidebar menu. The CLI > General page appears, and the number of controllers that the template is applied to automatically populates.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Command-Line Interface General template page appears (see Figure 10-61).

Figure 10-61 Command-Line Interface Template



Step 4 If you are adding a new template, provide a name that you are giving to this string of commands in the text box. If you are making modifications to an existing template, the Template Name text box cannot be modified.

Step 5 In the Commands page, enter the series of CLI commands.

Step 6 Select the **Refresh Config after Apply** check box to perform a refresh config on the controller after the CLI template is applied successfully.

Step 7 Click **Save** to save the CLI commands to the NCS database without applying to the selected controllers or **Apply to Controllers** to save the commands to the NCS database as well as apply to the selected controllers. If you click Apply to Controllers, choose the IP address of the controller to which you want to apply the template.

Note When the template is applied to the selected controllers, a status screen appears. If an error occurred while you applied the template, an error message is displayed. You can click the icon in the Session Output column to get the entire session output.

Note If the Controller Telnet credentials check fails or the Controller CLI template fails with invalid username and password even though the correct username and password are configured on the controller, check whether the controller has exceeded the number of CLI connections it can accept. If the connections have exceeded the maximum limit, then either increase the maximum allowed CLI sessions or terminate any pre-existing CLI sessions on the controller, and then retry the operation.

Configuring Location Configuration Templates

To add or modify a location setting template, follow these steps:

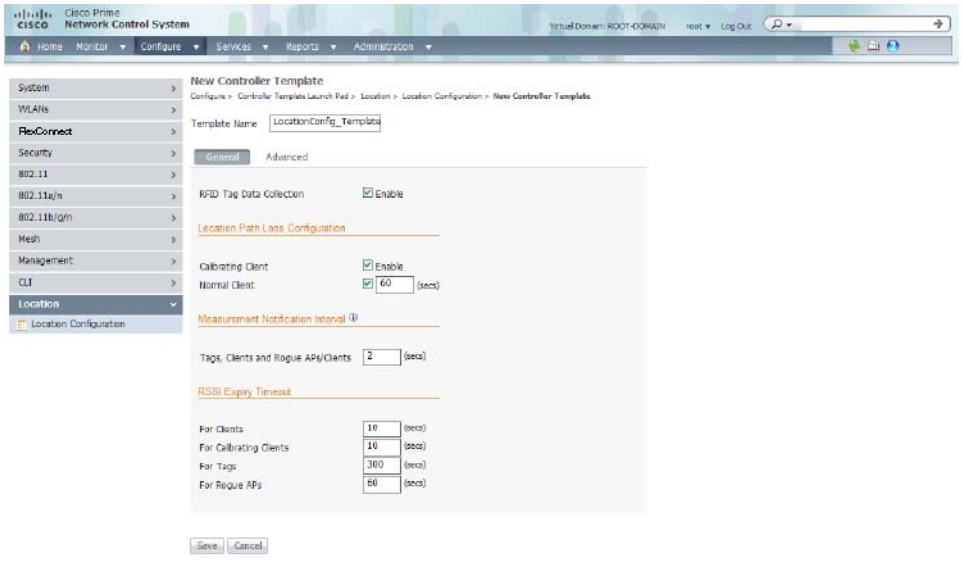
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Location > Location Configuration** or choose **Location > Location Configuration** from the left sidebar menu. The Location > Location Configuration page appears, and the number of controllers that the template is applied to automatically populates.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Location Configuration template page appears (see Figure 10-62).

Figure 10-62 Location Configuration Template



Step 4 Select the **RFID Tag Data Collection** check box to enable tag collection. Before the mobility services engine can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command **config rfid status enable** on the controllers.

Step 5 Select the **Calibrating Client** check box to enable calibration for the client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrating clients. Packets are transmitted on all channels. All access points irrespective of channel (and without a channel change) gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic.

Note To use all radios (802.11a/b/g/n) available, you must enable multiband in the Advanced page.

Step 6 Select the **Normal Client** check box to have a non-calibrating client. No S36 requests are transmitted to the client.

Note S36 and S60 are client drivers compatible with specific Cisco Compatible Extensions. S36 is compatible with CCXv2 or later. S60 is compatible with CCXv4 or later. For details, see the following URL: http://www.cisco.com/en/US/products/ps9806/products_qanda_item09186a0080af9513.shtml

Step 7 Specify how many seconds should elapse before notification of the found element (tags, clients, and rogue APs/clients).

Step 8 Enter the number of seconds after which RSSI measurements for clients should be discarded.

Step 9 Enter the number of seconds after which RSSI measurements for calibrating clients should be discarded.

Step 10 Enter the number of seconds after which RSSI measurements for tags should be discarded.

Step 11 Enter the number of seconds after which RSSI measurement for rogue access points should be discarded.

Step 12 Click the **Advanced** tab.

Step 13 Enter a value in seconds to set the RFID tag data timeout setting.

Step 14 Select the **Calibrating Client Multiband** check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled in the General group box.

Step 15 Click **Save**.

Configuring IPv6 Templates

This section contains the following topics:

Configuring Neighbor Binding Timers Templates

You can create or modify a template for configuring IPv6 Router Neighbor Binding Timers such as Down Lifetime, Reachable Lifetime, State Lifetime, and corresponding intervals.

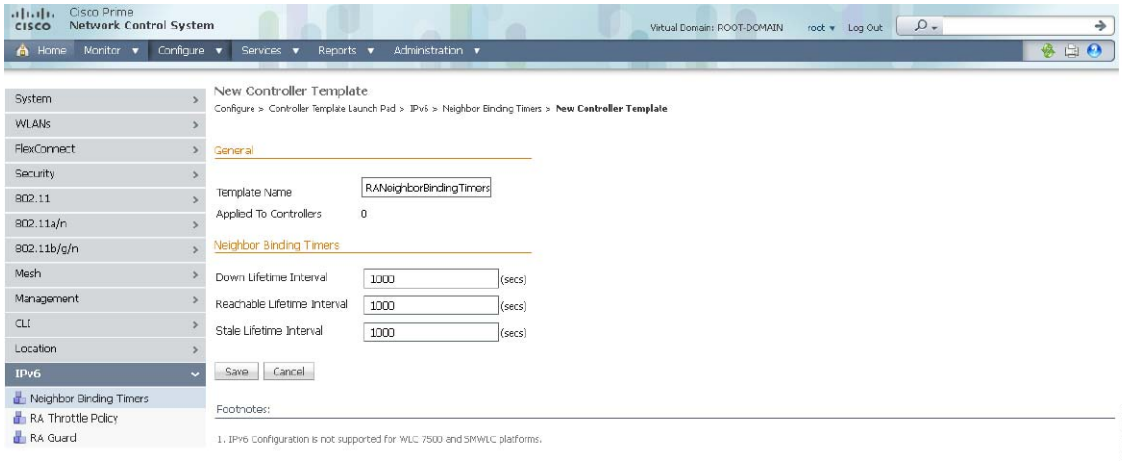
To configure a Neighbor Binding Timers template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Neighbor Binding Timers** or choose **IPv6 > Neighbor Binding Timers** from the left sidebar menu. The IPv6 > Neighbor Binding Timers page appears.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Neighbor Binding Timers template page appears (see Figure 10-62).

Figure 10-63 Neighbor Binding Timers Template



Step 4 Enter a template name in the text box.

Step 5 If you want to enable the down lifetime, select the **Enable** check box. If you have selected this check box, specify the value in the Down Lifetime Interval text box. This indicates the maximum time, in seconds, an entry learned from a down interface is kept in the binding table before the entry is deleted or proof is received that the entry is reachable.The range is 0 to 86,400 seconds, and the default value is 0.

Step 6 If you want to enable the reachable lifetime, select the **Enable** check box. If you have selected this check box, specify the value in the Reachable Lifetime Interval text box. This indicates the maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery protocol [NDP] inspection). After that, the entry is moved to stale.The range is 0 to 86,400 seconds, and the default value is 0.

Step 7 If you want to enable the stale lifetime, select the **Enable** check box. If you have selected this check box, specify the value in the Stale Lifetime Interval text box. This indicates the maximum time, in seconds, a stale entry is kept in the binding table before the entry is deleted or proof is received that the entry is reachable.The range is 0 to 86,400 seconds, and the default value is 0.

Step 8 Click **Save**.

Configuring RA Throttle Policy Templates

The RA Throttle Policy allows you to limit the amount of multicast Router Advertisements (RA) circulating on the wireless network. You can create or modify a template for configuring IPv6 Router Advertisement parameters such as RA Throttle Policy, Throttle Period, and other options.

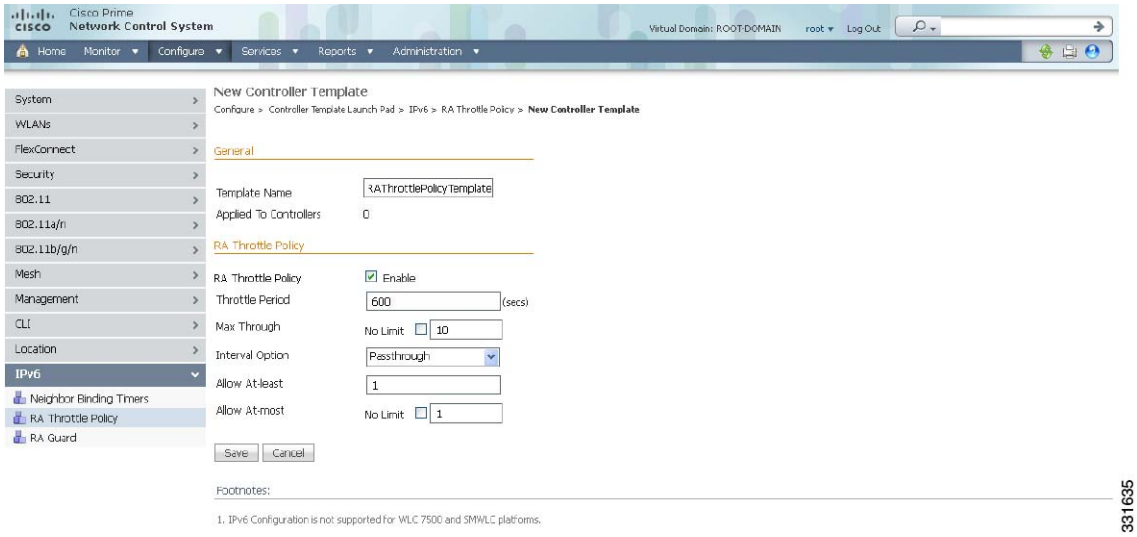
To configure a RA Throttle Policy template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **RA Throttle Policy** or choose **IPv6 > RA Throttle Policy** from the left sidebar menu. The IPv6 > RA Throttle Policy page appears.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The RA Throttle Policy template page appears (see Figure 10-62).

Figure 10-64 RA Throttle Policy Template



Step 4 Enter a template name in the text box.

Step 5 If you want to enable the down lifetime, select the **Enable** check box. If you have selected this check box, configure the following parameters:

- Throttle Period—Duration of the throttle period in seconds. The range is 10 to 86,400 seconds.
- Max Through—The number of RA that passes through over a period in seconds.
- Interval Option—Indicates the behavior in case of RA with an interval option.
- Allow At-least—Indicates the minimum number of RA not throttled per router.
- Allow At-most—Indicates the maximum number of RA not throttled per router.

Step 6 Click **Save**.

Configuring RA Guard Templates

RA Guard is a Unified Wireless solution used to drop RA from wireless clients. It is configured globally, and by default it is enabled. You can create or modify a template for configuring IPv6 Router Advertisement parameters.

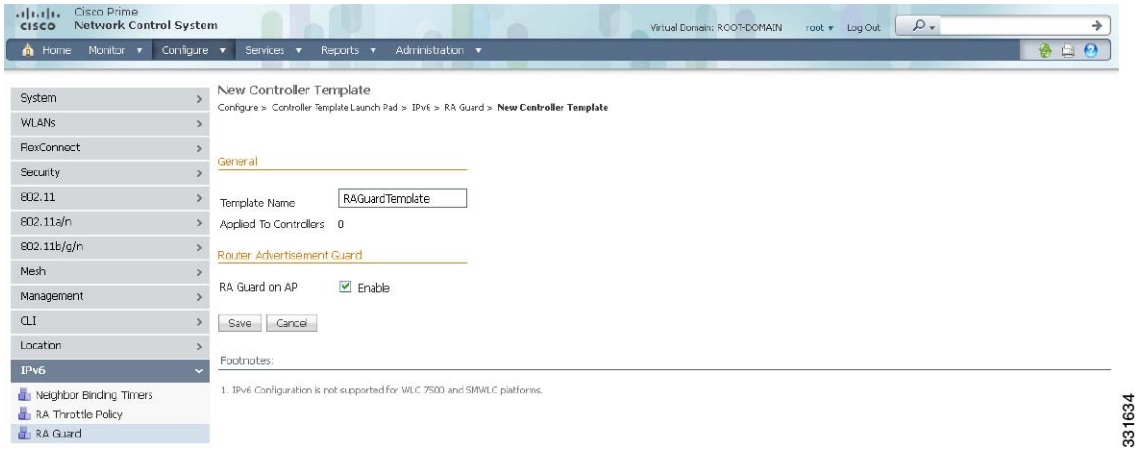
To configure an RA Guard template, follow these steps:

Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **RA Guard** or choose **IPv6 > RA Guard** from the left sidebar menu. The IPv6 > RA Guard page appears.

Step 3 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The RA Guard template page appears (see Figure 10-62).

Figure 10-65 RA Guard Template



Step 4 Enter a template name in the text box.

Step 5 If you want to enable the Router Advertisement Guard, select the **Enable** check box.

Step 6 Click **Save**.

Configuring AP Configuration Templates

This menu provides access to the access point templates summary details. Use the selector group box to access and configure the respective templates details.

Note Select the template name to view or edit parameters for current access point templates. View the applicable steps in Configuring a New Lightweight Access Point Template, page 10-138 for more information on access point template parameters.

This section contains the following topics:

Configuring Lightweight Access Point Templates

This section contains the following topics:

Configuring a New Lightweight Access Point Template

To configure a new Lightweight Access Point template, follow these steps:

Step 1 Choose **Configure > Lightweight AP Configuration Templates**.

Step 2 From the Select a command drop-down list, choose **Add Template**.

Step 3 Click **Go**.

Step 4 Enter a template name in the text box.

Step 5 Enter a template description in the text box.

Step 6 Click **Save**.

Step 7 Once loaded, the Lightweight AP Template Detail page appears. This section describes the Lightweight AP Template Detail page and contains the following topics:

AP Parameters Tab

Select the check box of the access point parameters that must be applied.

- Location—Enter the location in the Location text box.
- Admin Status—Select the **Admin and Enabled** check box to enable administrative status.

Note To conserve energy, access points can be turned off at specified times during non-working hours. Select the **Enabled** check box to allow access points to be turned on or off.

- AP Mode—From the drop-down list, choose one of the following:
  - **Local**—Default
  - **Monitor**—Monitor mode only.

    Note Choose **Monitor** to enable this access point template for Cisco Adaptive wIPS. Once Monitor is selected, select the **Enhanced WIPS Engine** check box and the Enabled check box. Then select the **AP Monitor Mode Optimization** check box and choose WIPS from the AP Monitor Mode Optimization drop-down list. For more information on Cisco Adaptive wIPS, see the "Configuring wIPS Profiles" section on page 8-237, or the "wIPS Policy Alarm Encyclopedia" section on page 17-1, and the "NCS Services" section on page 11-1.

  - FlexConnect—Cisco 1030 remote edge lightweight access point (REAP) used for Cisco 1030 IEEE 802.11a/b/g/n remote edge lightweight access points.

    Note FlexConnect must be selected to configure an OfficeExtend access point. When the AP mode is FlexConnect, FlexConnect configuration options display including the option to enable OfficeExtend AP and to enable Least Latency Controller Join. See the "Configuring FlexConnect" section on page 12-4 for more information.

  - Rogue Detector—Monitors the rogue access points but does not transmit or contain rogue access points.
  - Bridge
  - Sniffer—The access point "sniffs" the air on a given channel. It captures and forwards all the packets from the client on that channel to a remote machine that runs airopeek (a packet analyzer for IEEE 802.11 wireless LANs). It includes information on timestamp, signal strength, packet size, and so on. If you choose Sniffer as an operation mode, you are required to enter a channel and server IP address on the AP/Radio Templates 802.11b/g/n or 802.11a/n parameters tab.

    Note The sniffer feature can be enabled only if you are running AiroPeek, which is a third-party network analyzer software that supports decoding of data packets. For more information on AiroPeek, see http://www.wildpackets.com.

  - SE-Connect—This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.

    Note This option is displayed only if the access point is CleanAir-capable.

Note Changing the AP mode reboots the access point.

- Enhanced wIPS Engine—Select the **Enhanced wIPS engine** and the **Enabled** check box to enable.
- AP Monitor Mode Optimization—Choose **None** or **wIPS** from the drop-down list.
- AP Height (feet)—Enter the height of the access point (in feet) in the text box.
- Mirror Mode—Select the **Enabled** check box to enable mirror mode.
- Country Code—Select the appropriate country code from the drop-down list.

Note Changing the country code might cause the access point to reboot.

- Stats Collection Interval—Enter the stats collection interval in the text box.
- Cisco Discovery Protocol—Select the **Enabled** check box to enable Cisco Discovery Protocol.
- AP Failover Priority—Choose **Low**, **Medium**, **High**, or **Critical** from the drop-down list to indicate the access point failover priority. The default priority is low. See the "Setting AP Failover Priority" section on page 8-162 for more information.
- Pre-Standard 802.3af switches.
- Power Injector State—When enabled, this allows you to manipulate power injector settings through the NCS without having to go directly to the controllers. If the Enable Power Injector State is selected, power injector options appear.
- Power Injector Selection—Choose **installed** or **override** from the drop-down list.
- Injector Switch MAC Address—Enter the MAC address of the injector switch.
- Primary, Secondary, and Tertiary Controller IP—The Primary/Secondary/Tertiary Controller IP is the Management IP of the controller.
- Domain Name
- Domain Name Server IP Address—Domain Name Server IP and Domain Name can be configured only on APs which have static IP.
- Encryption—Select the **Encryption** check box to enable encryption.

Note Enabling or disabling encryption functionality causes the access point to reboot which then causes a loss of connectivity for clients.

Note DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security. Encryption is only available if the access point is connected to a 5500 series controller with a Plus license. Encryption is not available for all access point models.

Note Enabling encryption might impair performance.

- Rogue Detection—Select the check box to enable rogue detection. See the "Rogue Access Point Location, Tagging, and Containment" section on page 3-13 for more information on rogue detection.

Note Rogue detection is disabled automatically for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. For more information regarding OfficeExtend access points, see *Cisco Wireless LAN Controller Configuration Guide*.

- SSH Access—Select the **SSH Access** check box to enable SSH access.
- Telnet Access—Select the **Telnet Access** check box to enable Telnet access.

Note An OfficeExtend access point might be connected directly to the WAN which could allow external access if the default password is used by the access point. Because of this, Telnet and SSH access are disabled automatically for OfficeExtend access points.

- Link Latency—You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to the controller but is especially useful for FlexConnect access points, for which the link could be a slow or unreliable WAN connection. See the "Configuring Link Latency Settings for Access Points" section on page 8-213 for more information.

Note Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

- Reboot AP—Select the check box to enable a reboot of the access point after making any other updates.
- TCP Adjust MSS—Select the **TCP Adjust MSS** check box to enable TCP to adjust MSS.
- AP Failover Priority—Choose **Low**, **Medium**, **High**, or **Critical** from the drop-down list to indicate the access point failover priority. The default priority is low. See the "Setting AP Failover Priority" section on page 8-162 for more information.
- Controllers—Select the **Controllers** check box to enable the drop-down lists for the primary, secondary, and tertiary controller names.
- Group VLAN name—Choose the appropriate group VLAN name from the drop-down list.
- Override Global Username Password—Select the check box to enable an override for the global username/password. Enter and confirm the new access point username and password in the appropriate text boxes. See the "Configuring a Global Access Point Password" section on page 8-60 for more information on a global username and password.

Note In the System > AP Username Password page, you can set global credentials for all access points to inherit as they join a controller. These established credentials are displayed in the lower right of the AP Parameter tab page.

- Override Supplicant Credentials—Select the **Override Supplicant Credentials** check box to prevent this access point from inheriting the authentication username and password from the controller. The default value is unselected. The Override Supplicant Credentials option is supported in controller Release 6.0 and later.
  - In the Username, Password, and Confirm Password text boxes, enter the unique username and password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and whenever the access point joins a new controller.

Mesh Tab

Use the Mesh tab to set the following parameters for mesh access points:

- Bridge Group Name—Enter a bridge group name (up to 10 characters) in the text box.

  Note Bridge groups are used to logically group the mesh access points to avoid two networks on the same channel from communicating with each other.

  Note For mesh access points to communicate, they must have the same bridge group name.

  Note For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another.

- Data Rate (Mbps)—Choose the data rate for the backhaul interface from the drop-down list. Data rates available are dictated by the backhaul interface. The default rate is 18 Mbps.

  Note This data rate is shared between the mesh access points and is fixed for the whole mesh network.

  Note Do not change the data rate for a deployed mesh networking solution.

- Ethernet Bridging—Select the **Enable** check box. From the Ethernet Bridging drop-down list, enable Ethernet bridging for the mesh access point.
- Role—Choose the role of the mesh access point from the drop-down list (**MAP** or **RAP**). The default setting is MAP.

  Note An access point in a mesh network functions as either a root access point (RAP) or mesh access point (MAP).

802.11a/n Tab

Select the check boxes of the 802.11a/n parameters that must be applied:

- Channel Assignment
- Admin Status
- Antenna Mode
- Antenna Diversity
- Antenna Name

- Power Assignment
- WLAN Override
- 11n Antenna Selection
- CleanAir

802.11a SubBand Tab

Select the 802.11a Sub Band options (for either 4.9 or 5.8 parameters) that must be applied:

Note Options are disabled unless the check box to the left of the field is selected.

- Admin Status
- Channel Assignment—Select the check box and then choose the appropriate channel from the drop-down list.

  Note The channel number is validated against the radio list of supported channels.

- Power Assignment—Select the check box and then choose the appropriate power level from the drop-down list.

  Note The power level is validated against the radio list of supported power levels.

- WLAN Override—Select the check box and then choose **Disable** or **Enable** from the drop-down list.

  Note The access point must be reset for the WLAN override change to take effect.

- Antenna Type—Select the check box and then choose the antenna type from the drop-down list.
- Antenna Name—Select the **Antenna Type** check box and then choose the applicable antenna name from the drop-down list.

  Note Not all antenna models are supported by radios of different access point types.

802.11b/g/n Tab

Select the check box of the 802.11b/g/n parameters that must be applied:

- Channel Assignment
- Admin Status
- Antenna Mode
- Antenna Diversity
- Antenna Name
- Power Assignment
- WLAN Override

- Tracking Optimized Monitor Mode
- 11n Antenna Selection
- CleanAir

CDP Tab

- In the Cisco Discovery Protocol on Ethernet Interfaces group box, select the check boxes for the slots of Ethernet interfaces for which you want to enable CDP.
- In the Cisco Discovery Protocol on Radio Interfaces group box, select the slots of Radio interfaces for which you want to enable CDP.

FlexConnect Tab

- FlexConnect Configuration—Select the check box to enable FlexConnect configuration (including VLAN support, native VLAN ID, and profile name VLAN mappings).

  Note These options are only available for access points in FlexConnect mode.

  – OfficeExtend—The default is Enabled.

    Note Unselecting the check box simply disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point configuration and return it to factory default settings, click **Clear Config** at the bottom of the access point details page. If you want to clear only the access point personal SSID, click Reset Personal SSID at the bottom of the access point details page. See the "Restoring Factory Defaults" section on page 8-34 for more information.

    Note When you select Enable for the OfficeExtend AP, several configuration changes automatically occur including: encryption and link latency are enabled; rogue detection, SSH access, and Telnet access are disabled.

    Note When you enable the OfficeExtend access point, you must configure at least one primary, secondary, and tertiary controller (including name and IP address).

  – Least Latency Controller Join—When enabled, the access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.

    Note The access point only performs this search once when it initially joins the controller. It does not recalculate the latency measurements of primary, secondary, and tertiary controllers once joined to see if the measurements have changed.

  – VLAN Support
  – Native VLAN ID

Note The valid native VLAN ID range is 1—4094. If you are changing the mode to REAP and if the access point is not already in REAP mode, then all other REAP parameters are not applied on the access point.

Click the **Show/Add VLAN ACL Mapping** link to add or delete a VLAN ID and map it to Ingress ACL and Egress ACL.

- VLAN ID ACL Mapping—Enter a VLAN ID and choose the Ingress and Egress ACLs from the drop-down list boxes to map to the VLAN ID specified.

Click the **Show/Add WebAuth ACL Mapping** link to add or delete a WLAN Profile and WebAuth ACL mapping.

- WLAN Profile to ACL Mapping— Choose the WLAN Profile and WebAuth ACL from the drop-down list boxes to add a WebAuth ACL mapping.

Click the **Show/Add WebPolciy ACL** link to add or delete a Web Policy ACL.

Select APs Tab

Use the Search APs drop-down list to search for Last Applied AP(s), Scheduled AP(s), All, All Mesh MAP AP(s), All Mesh RAP AP(s), By Controller (choose the controller from the drop-down list), By Controller Name (choose the controller name from the drop-down list), By Floor Area (choose the campus, building, and floor area from the drop-down lists), By Outdoor Area (choose the campus and the outdoor area from the drop-down lists), By Model (choose the model from the drop-down list), By AP MAC Address (enter the MAC address), By AP Name (enter the complete AP name or starting characters of the AP name), and By AP IP Address Range (enter the IP address).

Note The input text for IP address search can be of two formats X.X.X.* or X.X.X.[0-255]. For example, 10.10.10.* or 10.10.10.[20-50] searches the APs in 10.10.10.10 to 10.10.10.50 IP address range.

Note The All Applied APs and Scheduled APs search filters list the last 24 hours AP data.

Note The AP(s) unassigned to Map(s) search filter lists the APs that have not yet been assigned to any maps.

- Click **Save** to save the parameters selections.
- Click **Apply** to save and apply the AP/Radio parameters to the selected access points from the search.

Apply/Schedule Tab

Allows you to save the current template, apply the current template immediately, or schedule the current template to start the provisioning at the applicable time.

- Save—Click **Save** to save the current template configuration.
- Apply—Click **Apply** to save the template and start the provisioning of the template to selected access points.

Note This provisioning process continues until completed even if you leave the page and log out of the NCS.

- Schedule—Allows you to configure and start the provisioning at a scheduled time.
  - Enable schedule—Select the **Enable schedule** check box to activate the scheduling function.
  - Start Date—Enter a starting date in the text box or use the calendar icon to select a start date.
  - Start Time—Select the starting time using the hours and minutes drop-down lists.
  - Recurrence—Select from no recurrence, hourly, daily, or weekly to determine how often this provisioning occurs. Enter how often (in days) the provisioning is to occur.
  - Schedule—Click **Schedule** to start the provisioning at the scheduled time.

Report Tab

Displays all recently applied reports including the apply status and the date and time the apply was initiated. The following information is provided for each individual access point:

- Status—Indicates success, partial failure, failure, or not initiated. For failed or partially failed provisioning, click **Details** to view the failure details (including what failed and why it failed).
- Ethernet MAC—Indicates the Ethernet MAC address for the applicable access point.
- Controller—Indicates the controller IP address for the applicable access point.
- Map—Identifies a map location for the access point.

Note Click the **click here** link at the bottom of the Report page to view scheduled task reports.

Editing a Current Lightweight Access Point Template

To edit a current Lightweight Access Point Template, follow these steps:

Step 1 Choose **Configure > Lightweight AP Configuration Templates**.

Step 2 Click the applicable template in the Template Name column.

Step 3 Edit the necessary parameters on the following tabs:

- AP Parameters—Select the check box of the access point parameters that must be applied.
- Mesh
- 802.11a/n Parameters—Select the check box of the 802.11a/n parameters that must be applied.
- 802.11b/g/n Parameters—Select the check box of the 802.11b/g/n parameters that must be applied.
- Select APs
  - Use the Search APs drop-down list to search for Last Applied APs, All APs, All MAP(s), or All RAP(s).
  - Click **Save** to save the parameters selections.

- Click **Apply** to save and apply the AP/Radio parameters to the selected access points from the search.
- Apply Report—Displays the reports from the applied template.

Configuring Autonomous Access Point Templates

The Configuring > Autonomous Access Point Templates page allows you to configure CLI templates for autonomous access points.

This section contains the following topics:

Configuring a New Autonomous Access Point Template

To configure a new Autonomous Access Point template, follow these steps:

Step 1 Choose **Configure > Autonomous AP Configuration Templates**.

Step 2 From the Select a command drop-down list, choose **Add Template**.

Step 3 Click **Go**.

Step 4 Enter a Template Name.

Step 5 Enter the applicable CLI commands.

Note Do not include any show commands in the CLI commands text box. The show commands are not supported.

Step 6 Click **Save**.

Applying an AP Configuration Template to an Autonomous Access Point

To apply an AP Configuration template to an autonomous access point, follow these steps:

Step 1 Choose **Configure > Autonomous AP Configuration Templates**.

Step 2 Click the template name link to select a template and apply it to the an autonomous access point. The New Autonomous AP Configuration template page appears.

Step 3 Enter a **Template Name**.

Step 4 Enter the applicable CLI commands.

Step 5 Click **Save**.

Step 6 Click **Apply to Autonomous Access Points**. The Apply to Autonomous Access Points page appears.

Step 7 Select the desired autonomous access point.

Step 8 Click **OK**.

Note Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the Autonomous AP. If this check box is not selected, any errors encountered while applying a command in the template to a Autonomous AP causes the rest of the commands to be not applied.

Viewing Template Results

To view the results when you apply an Autonomous AP Configuration template to an access point, follow these steps:

Step 1 Choose **Configure > AP Configuration Templates > Autonomous AP**.

Step 2 Click the template name link to select a template and apply it to the an autonomous access point. The Autonomous AP Configuration template page appears.

Step 3 Enter a **Template Name**.

Step 4 Enter the applicable CLI commands.

Step 5 Click **Save**.

Step 6 Click **Apply to Autonomous Access Points**. The Apply to Autonomous Access Points page appears.

Step 7 Select the desired autonomous access point.

Step 8 Click **OK**. The Template Results page appears. The following parameters appear:

- IP Address —IP address of the access point.
- AP Name—The name of the access point.
- Apply Status—Indicates success, failure, initiated or not initiated.
- Operation Status—Displays the operational status: Success or Failure.
- Reason—Indicates the reasons for failure.
- Session Output

Configuring Switch Location Configuration Templates

You can configure the location template for a switch using the Switch Location Configuration template.

To configure a location template for a switch, follow these steps:

Step 1 Choose **NCS > Configure > Switch Location Configuration Template**.

The Switch Location Configuration template page appears.

Step 2 From the Select a command drop-down list, choose **Add Template**, and click **Go**.

The New Template page appears.

Table 10-4 lists the fields in the New Template page.

Field	Description
General	
Template Name	Name of the template.
Map Location	
Campus	Choose a campus for the map location for a switch/switch port.
Building	Choose a building for the map location for a switch/switch port.
Floor	Choose a floor for the map location for a switch/switch port.
Import	Imports the civic information for the campus, building, and floor selected.
ELIN and Civic Location	
ELIN	The Emergency Location Identification Number.
Civic Address tab	The available civic address information for the switch/switch port.
Advanced tab	Detailed information about the switch/switch port location.
NMSP	Select or unselect this check box to enable or disable NMSP for the switch.
Buttons	
Save	Saves the template.
Cancel	Discards the template creation.

Configuring Autonomous AP Migration Templates

This section contains the following topic:

Migrating an Autonomous Access Point to a Lightweight Access Point

To make a transition from an Autonomous solution to a Unified architecture, autonomous access points must be converted to lightweight access points. The migration utility is available in the Configure > Autonomous AP Migration Templates page where existing templates are listed.

The Autonomous AP Migration Templates list page displays the following information:

- Name—The template name.
- Description—The description of template.
- AP Count—The number of autonomous access points selected for migration.
- Schedule Run—The time at which the task is scheduled to run.
- Status—Indicates one of the following task statuses:
  - Not initiated—The template is yet to start the migration and starts at the scheduled time.
  - Disabled—The template is disabled and does not run at the scheduled time. This is the default state for a template when it is created without selecting any autonomous access points.
  - Expired—The template did not run at the scheduled time (this might be due to the NCS server being down).
  - Enabled—The template is yet to start the migration and starts at the scheduled time.
  - In progress—The template is currently converting the selected autonomous access points to CAPWAP.
  - Success—The template has completed the migration of autonomous access point to CAPWAP successfully.
  - Failure—The template failed to migrate all the selected autonomous access point to CAPWAP. You can check the detailed status about the failures by using the View Migration Status page.
  - Partial Success—The template failed to migrate a subset of the selected autonomous access point to CAPWAP. You can check the detailed status about the failures by using the View Migration Status page.

Note In any of these states, you can edit the template by clicking the **Name** link.

Note Once an access point is converted to lightweight, the previous status or configuration of the access point is not retained.

From the Select a command drop-down list, the following functions can be performed:

- Add Template—Allows you to provide necessary information for migration.
- Delete Templates—Allows you to delete a current template.
- View Migration Report—Allows you to view information such as AP address, migration status (in progress or fail), timestamp, and a link to detailed logs.
- View Current Status—Allows you to view the progress of the current migration (updated every three seconds).

Note When you migrate an already-managed autonomous access point to lightweight, its location and antenna information is migrated as well. You do not need to reenter the information. The NCS automatically removes the autonomous access point after migration.

- View Migration Analysis Summary—Lists the pass or fail status as required for an access point conversion. Only those access points with all criteria as pass are eligible for conversion.

Note The Migration Analysis option does not run during discovery by default. If you prefer to run the migration analysis during discovery, choose **Administration > Settings > CLI Session** to enable this option.

Note The NCS also supports the migration of autonomous access point to CAPWAP access point.

Editing Current Autonomous AP Migration Templates

To edit a current migration template, follow these steps:

Step 1 Choose **Configure > Autonomous AP Migration Templates**.

Step 2 Click the migration template in the Name column.

Step 3 Edit the necessary parameters:

- General
  - Name—Indicates the user-defined name of the migration template.
  - Description—Enter a brief description to help you identify the migration template.
- Upgrade Options
  - DHCP Support—Click to enable Dynamic Host Configuration Protocol support. This ensures that after the conversion every access point gets an IP from the DHCP server.
  - Retain AP HostName—Click to enable retention of the same hostname for this access point.

Note The hostname is retained in the CAPWAP, only when you are migrating the AP to CAPWAP for the first time. It might not be retained if you are upgrading an AP for several times. The CAPWAP access points hostname is set to default if autonomous access points hostname has more than 32 characters.

Note If you upgrade the access points to LWAPP from 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, 12.3(11)JA3 autonomous images, the converted access points might not retain their Static IP Address, Netmask, Hostname and Default Gateway.

  - Migrate over WANLink—If you enable this option, the *env_vars* file stores the remote TFTP server location. This information is copied to the AP. If this option is not selected, then the NCS internal TFTP server is used to copy the *env_vars* file to AP.
  - DNS Address—Enter the DNS address.
  - Domain Name—Enter the domain name.
- Controller Details

Note Ensures that the access point authorization information (SSC) can be configured on this controller and the converted access points can join.

  - Controller IP
  - AP Manager IP
  - User Name
  - Password
- TFTP Details
  - TFTP Server IP
  - File Path
  - File Name
- Schedule Details
  - Apply Template
  - Notification (Optional)

Step 4 Click **Save**.

Viewing the Migration Analysis Summary

To view the Migration Analysis Summary, follow these steps:

Note You can also view the migration analysis summary by choosing **Tools > Migration Analysis**.

Step 1 Choose **Configure > Autonomous AP Migration Templates**.

Step 2 Choose **View Migration Analysis Summary** from the Select a command drop-down list, and click **Go**. The Migration Analysis Summary page appears.

The autonomous access points are eligible for migration only if all the criteria have a pass status. A red X designates ineligibility, and a green checkmark designates eligibility. These columns represent the following:

- Privilege 15 Criteria—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.
- Software Version Criteria—Conversion is supported only in Cisco IOS Release 12.3(7)JA excluding 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, and 12.3(11)JA3.
- Role Criteria—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
  - root
  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only
- Radio Criteria—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.

Adding/Modifying a Migration Template

If you want to add a migration template, choose **Add Template** from the Select a command drop-down list in the Configure > Autonomous AP Migration Templates page.

To modify an existing template, click the template name from the summary list.

Enter or modify the following migration parameters:

General

- Name—User-defined name of this migration template.
- Description—Brief description to help you identify the migration template.

Upgrade Options

- DHCP Support—Ensures that after the conversion every access point gets an IP from the DHCP server.
- Retain AP HostName—Allows you to retain the same hostname for this access point.
- Migrate over WANLink—Increases the default timeouts for the CLI commands executed on the access point.
- DNS Address
- Domain Name

Controller Details

Note Ensure that the access point authorization information (SSC) can be configured on this controller and the converted access points can join.

- Controller IP—Enter the IP address of the WLAN controller you are wanting to add to the newly migrated access point.
- AP Manager IP—Specify the controller the access point should join by entering the access point manager IP address.

  Note For SSC-enabled access points, this IP address must be the same as the controller IP field. For MIC-enabled access points, the IP addresses need not match.

- User Name—Enter a valid username for login of the WLAN controller.
- Password—Enter a valid password for this username used during WLAN controller login.

TFTP Details

The NCS provides its own TFTP and FTP server during the installation and setup.

- TFTP Server IP—Enter the IP address of the NCS server.
- File Path—Enter the TFTP directory which was defined during the NCS setup.
- File Name—Enter the CAPWAP conversion file defined in the TFTP directory during the NCS setup (for example, c1240-rcvk9w8-tar.123-11JX1.tar).

Schedule Details

This group box enables you to specify scheduling options for migration templates.

- Apply Template—Choose an option by which you want to apply the template for migration.
  - Now—Choose this option to run the migration task immediately.
  - Schedule for later date/time—If you plan to schedule the migration at a later time, enter the Schedule parameters. Enter a date in the text box, or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists. The report begins running on this data and at this time.
- (Optional) Notification—Enter the e-mail address of recipient to send notifications via e-mail.

Note To receive e-mail notifications, configure the NCS mail server in the Administration > Settings > Mail Server Configuration page.

- Click **Save**.

Once a template is added in the NCS, the following additional buttons appear:

- Select APs—Choosing this option provides a list of autonomous access points in the NCS from which to choose the access points for conversion. Only those access points with migration eligibility as *pass* can be chosen for conversion.
- Select File—To provide CSV information for access points intended for conversion.

Copying a Migration Template

To copy a migration template, follow these steps:

Step 1 Choose **Configure > Autonomous AP Migration Templates**.

Step 2 Select the check box of the template you want to copy, and then choose **Copy Template** from the Select a command drop-down list.

Step 3 Click **Go**.

Step 4 Enter the name for the new template to which you want to copy the current template.

Deleting Migration Templates

To delete migration templates, follow these steps:

Step 1 Choose **Configure > Autonomous AP Migration Templates**.

Step 2 Select the check box(es) of the template(s) you want to delete, and then choose **Delete Templates** from the Select a command drop-down list.

Step 3 Click **Go**.

Step 4 Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the template.

Viewing the Current Status of Cisco IOS Access Points

Select **View Current Status** from the Select a command drop-down list in the Autonomous AP Migration Templates page to view the status of Cisco IOS access point migration.

The following information is displayed:

- IP Address—IP address of the access point.
- Status—Current status of the migration.
- Progress—Summary of the migration progress.

Disabling Access Points that are Ineligible

If an autonomous access point is labelled as ineligible for conversion, you can disable it.

CHAPTER 12

Configuring FlexConnect

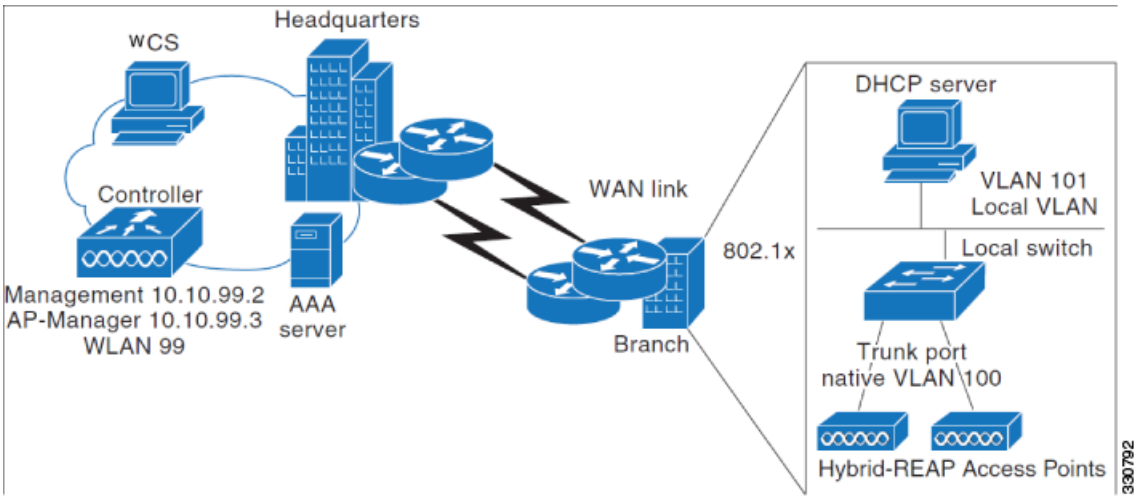
This chapter describes FlexConnect and explains how to configure this feature on controllers and access points. It contains the following sections:

Information About FlexConnect

FlexConnect is a solution for branch office and remote office deployments. It enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. There is no deployment restriction on the number of FlexConnect access points per location. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller.

FlexConnect is supported only on the 1130AG, 1240AG, 1142 and 1252 access points and on the 2000 and 4400 series controllers, the Catalyst 3750G Integrated Wireless LAN Controller Switch, the Cisco WiSM, the Controller Network Module for Integrated Services Routers, and the controller within the Catalyst 3750G Integrated Wireless LAN Controller Switch. Figure 12-1 illustrates a typical FlexConnect deployment.

Figure 12-1 FlexConnect Deployment



This section contains the following topics:

FlexConnect Authentication Process

When a FlexConnect access point boots up, it looks for a controller. If it finds one, it joins the controller, downloads the latest software image from the controller and configuration information, and initializes the radio. It saves the downloaded configuration in non-volatile memory for use in standalone mode.

A FlexConnect access point can learn the controller IP address in one of the following ways:

- If the access point has been assigned an IP address from a DHCP server, it discovers a controller through the regular CAPWAP discovery process [Layer 3 broadcast, over-the-air provisioning (OTAP), DNS, or DHCP option 43.]

Note OTAP does not work on the first boot out of the box.

- If the access point has been assigned a static IP address, it can discover a controller through any of the CAPWAP discovery process methods except DHCP option 43. If the access point cannot discover a controller through Layer 3 broadcast or OTAP, we recommend DNS resolution. With DNS, any access point with a static IP address that knows of a DNS server can find at least one controller.
- If you want the access point to discover a controller from a remote network where CAPWAP discovery mechanisms are not available, you can use priming. This method enables you to specify (through the access point command-line interface) the controller to which the access point is to connect.

When a FlexConnect access point can reach the controller (referred to as *connected mode*), the controller assists in client authentication. When a FlexConnect access point cannot access the controller, the access point enters standalone mode and authenticates clients by itself.

Note The LEDs on the access point change as the device enters different FlexConnect modes. See the hardware installation guide for your access point for information on LED patterns.

When a client associates to a FlexConnect access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration. With respect to client authentication (open, shared, EAP, web authentication, and NAC) and data packets, the WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

- **central authentication, central switching**—In this state, the controller handles client authentication, and all client data tunnels back to the controller. This state is valid only in connected mode.
- **central authentication, local switching**—In this state, the controller handles client authentication, and the FlexConnect access point switches data packets locally. After the client authenticates successfully, the controller sends a configuration command with a new payload to instruct the FlexConnect access point to start switching data packets locally. This message is sent per client. This state is applicable only in connected mode.
- **local authentication, local switching**—In this state, the FlexConnect access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

  Local authentication is useful where you cannot maintain the criteria a remote office setup of minimum bandwidth of 128 kbps with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local switching, the authentication capabilities are present in the access point itself. Thus local authentication reduces the latency requirements of the branch office.

Note Local authentication can only be enabled on the WLAN of a FlexConnect access point that is in local switching mode.

  Local authentication is not supported in the following scenarios:

  - Guest Authentication cannot be done on a FlexConnect local authentication enabled WLAN.
  - RRM information is not available at the controller for the FlexConnect local authentication enabled WLAN.
  - Local radius is not supported.
  - Once the client has been authenticated, roaming is only be supported after the WLC and the other FlexConnects in the group are updated with the client information.
- **authentication down, switching down**—In this state, the WLAN disassociates existing clients and stops sending beacon and probe responses. This state is valid only in standalone mode.
- **authentication down, local switching**—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

When a FlexConnect access point enters standalone mode, WLANs that are configured for open, shared, WPA-PSK, or WPA2-PSK authentication enter the “local authentication, local switching” state and continue new client authentications. Other WLANs enter either the “authentication down, switching down” state (if the WLAN was configured to central switching) or the “authentication down, local switching” state (if the WLAN was configured to local-switch).

When a FlexConnect access point enters standalone mode, it disassociates all clients that are on centrally switched WLANs. For 802.1X or web-authentication WLANs, existing clients are not disassociated, but the FlexConnect access point stops sending beacons when the number of associated clients reaches zero (0). It also sends disassociation messages to new clients associating to 802.1X or web-authentication WLANs. Controller-dependent activities such as 802.1X authentication, NAC, and web authentication (guest access) are disabled, and the access point does not send any Intrusion Detection System (IDS) reports to the controller. Furthermore, most Radio Resource Management (RRM) features (such as neighbor discovery; noise, interference, load, and coverage measurements; use of the neighbor list; and rogue containment and detection) are disabled. However, a FlexConnect access point supports dynamic frequency selection in standalone modes.

Note If your controller is configured for Network Access Control (NAC), clients can associate only when the access point is in connected mode. When NAC is enabled, you need to create an unhealthy (or quarantined) VLAN so that the data traffic of any client that is assigned to this VLAN passes through the controller, even if the WLAN is configured for local switching. After a client is assigned to a quarantined VLAN, all of its data packets are centrally switched.

The FlexConnect access point maintains client connectivity even after entering standalone mode. However, once the access point reestablishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and reallows client connectivity.

FlexConnect Guidelines

Keep the following guidelines in mind when using FlexConnect:

- A FlexConnect access point can be deployed with either a static IP address or a DHCP address. In the case of DHCP, a DHCP server must be available locally and must be able to provide the IP address for the access point at bootup.
- FlexConnect supports a 500-byte maximum transmission unit (MTU) WAN link at minimum.
- Roundtrip latency must not exceed 300 milliseconds (ms) between the access point and the controller, and CAPWAP control packets must be prioritized over all other traffic. In cases where you cannot achieve this, you can configure the access point to perform local authentication. See the "FlexConnect Authentication Process" section on page 12-2 for more information about FlexConnect local authentication using local authentication and local switching.
- The controller can send multicast packets in the form of unicast or multicast packets to the access point. In FlexConnect mode, the access point receives multicast packets only in unicast form.
- FlexConnect supports CCKM full authentication but not CCKM fast roaming.
- FlexConnect supports a 1-1 network address translation (NAT) configuration. It also supports Port Address Translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option.
- VPN, IPsec, L2TP, PPTP, Fortress authentication, and Cranite authentication are supported for locally switched traffic, provided that these security types are accessible locally at the access point.

Configuring FlexConnect

To configure FlexConnect, you must follow the instructions in this section in the order provided. This section contains the following topics:

Configuring the Switch at the Remote Site

To prepare the switch at the remote site, follow these steps:

Step 1 Attach the access point that is enabled for FlexConnect to a trunk or access port on the switch.

Note The following sample configuration shows the FlexConnect access point connected to a trunk port on the switch.

Step 2 See the sample configuration that follows to configure the switch to support the FlexConnect access point.

In this sample configuration, the FlexConnect access point is connected to trunk interface FastEthernet 1/0/2 with native VLAN 100. The access point needs IP connectivity on the native VLAN. The remote site has local servers/resources on VLAN 101. A DHCP pool is created in the local switch for both VLANs in the switch. The first DHCP pool (NATIVE) is used by the FlexConnect access point, and the second DHCP pool (LOCAL-SWITCH) is used by the clients when they associate to a WLAN that is locally switched. The bolded text in the sample configuration illustrates these settings.

Note The addresses in this sample configuration are for illustration purposes only. The addresses that you use must fit into your upstream network.

```
ip dhcp pool NATIVE
   network 10.10.100.0 255.255.255.0
   default-router 10.10.100.1
!
ip dhcp pool LOCAL-SWITCH
   network 10.10.101.0 255.255.255.0
   default-router 10.10.101.1
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 10.10.98.2 255.255.255.0
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
switchport mode trunk
 spanning-tree portfast
!
interface Vlan100
 ip address 10.10.100.1 255.255.255.0
 ip helper-address 10.10.100.1
!
```

```
interface Vlan101
 ip address 10.10.101.1 255.255.255.0
 ip helper-address 10.10.101.1
end
```

Configuring the Controller for FlexConnect

This section provides the procedure for configuring the controller for FlexConnect. The controller configuration for FlexConnect consists of creating centrally switched and locally switched VLANs. This procedure uses the following three WLANs as examples.

WLAN	Security	Switching	Interface Mapping (VLAN)
employee	WPA1+WPA2	Central	management (centrally switched VLAN)
employee-local	WPA1+WPA2 (PSK)	Local	101 (local switched VLAN)
guest-central	Web authentication	Central	management (centrally switched VLAN)

To create a centrally switched WLAN, follow these steps. In our example, this is the first WLAN (employee).

Step 1 Choose **Configure** > **Controllers**.

Step 2 Click the desired controller in the IP Address column.

Step 3 Choose **WLANs** > **WLAN Configuration** to access the WLAN Configuration page.

Step 4 Choose **Add a WLAN** from the Select a command drop-down list, and click **Go**.

Note Cisco access points can support up to 16 WLANs per controller. However, some Cisco access points do not support WLANs that have a WLAN ID greater than 8. In such cases, when you attempt to create a WLAN, you get a message that says "Not all types of AP support WLAN ID greater than 8, do you wish to continue?". Clicking OK creates a WLAN with the next available WLAN ID. However, if you delete a WLAN that has a WLAN ID less than 8, then the WLAN ID of the deleted WLAN is applied to the next created WLAN.

Step 5 If you want to apply a template to this controller, choose a template name from the drop-down list. The fields populate according to how the template is set. If you want to create a new WLAN template, click the **click here** link to be redirected to the template creation page (see the "Configuring WLAN Templates" section on page 10-22).

Step 6 Modify the configuration parameters for this WLAN. In our employee WLAN example, you must choose **WPA1+WPA2** from the Layer 2 Security drop-down list.

Step 7 Be sure to enable this WLAN by selecting the **Status** check box under General Policies.

Note If NAC is enabled and you created a quarantined VLAN for use with this, make sure to select it from the Interface drop-down list under General Policies. Also, select the **Allow AAA Override** check box to ensure that the controller validates a quarantine VLAN assignment.

Step 8 Click **Save** to commit your changes.

Step 9 Follow these steps to create a locally switched WLAN. In our example, this is the second WLAN (employee-local).

a. Follow the substeps in Step to create a new WLAN. In our example, this WLAN is named "employee-local."

b. Click a WLAN ID from the original WLAN page to move to a WLANs edit page. Modify the configuration parameters for this WLAN. In our employee WLAN example, you need to choose **WPA1+WPA2** from the Layer 2 Security drop-down list. Make sure you choose **PSK authentication key management** and enter a preshared key.

Note Make sure you enable this WLAN by selecting the **Admin Status** check box. Also, make sure you enable local switching by selecting the **FlexConnect Local Switching** check box. When you enable local switching, any FlexConnect access point that advertises this WLAN is able to locally switch data packets (instead of tunneling them to the controller).

Note For FlexConnect access points, the interface mapping at the controller for WLANs configured for FlexConnect local switching is inherited at the access point as the default VLAN tagging. This can be easily changed per SSID and per FlexConnect access point. Non-FlexConnect access points tunnel all traffic back to the controller, and VLAN tagging is dictated by each interface mapping of the WLAN.

c. Click **Save** to commit your changes.

Step 10 Follow these steps if you also want to create a centrally switched WLAN that is used for guest access. In our example, this is the third WLAN (guest-central). You might want to tunnel guest traffic to the controller so that you can exercise your corporate data policies for unprotected guest traffic from a central site.

a. Follow the substeps in Step to create a new WLAN. In our example, this WLAN is named "guest-central."

b. In the WLANs Edit page, modify the configuration parameters for this WLAN. In our employee WLAN example, you must choose **None** from the Layer 2 Security and Layer 3 Security drop-down lists on the Security tab, select the **Web Policy** check box, and make sure **Authentication** is selected.

Note If you are using an external web server, you must configure a preauthentication access control list (ACL) on the WLAN for the server and then choose this ACL as the WLAN preauthentication ACL.

c. Make sure you enable this by selecting the **Status** check box.

d. Click **Save** to commit your changes.

e. If you want to customize the content and appearance of the login page that guest users see the first time they access this, follow the instructions in the "Configuring a Web Authentication Template" section on page 10-68.

f. To add a local user to this WLAN, choose **Configure > Controller Template Launch Pad**.

g. Choose **Security > Local Net Users** from the left sidebar menu.

h. When the Local Net Users page appears, choose **Add Template** from the Select a command drop-down list, and click **Go**.

i. Unselect the **Import from File** check box.

j. Enter a username and password for the local user.

k. From the Profile drop-down list, choose the appropriate SSID.

l. Enter a description of the guest user account.

m. Click **Save**.

Step 11 See the "Configuring an Access Point for FlexConnect" section on page 12-8 to configure two or three access points for FlexConnect.

Configuring an Access Point for FlexConnect

This section provides instructions for configuring an access point for FlexConnect.

To configure an access point for FlexConnect, follow these steps:

Step 1 Make sure that the access point has been physically added to your network.

Step 2 Choose **Configure > Access Points**.

Step 3 Choose which access point you want to configure for FlexConnect by clicking it in the AP Name list. The Access Point Detail page appears.

The last field listed in the Inventory Information group box indicates whether this access point can be configured for FlexConnect. Only the 1130AG and 1240AG access points support FlexConnect.

Step 4 Verify that the AP Mode field displays *FlexConnect*. If it does not, continue to Step 5. If FlexConnect is showing as supported, skip to Step 9.

Step 5 Choose **Configure > AP Configuration Templates > Lightweight AP** or **Autonomous AP**.

Step 6 Choose which access point you want to configure for FlexConnect by clicking it in the AP Name list. The Lightweight AP Template Detail page appears.

Step 7 Select the **FlexConnect Mode supported** check box. Enabling this configuration allows you to view all profile mappings.

Note If you are changing the mode to FlexConnect and if the access point is not already in FlexConnect mode, all other FlexConnect parameters are not applied on the access point.

Step 8 Select the **VLAN Support** check box and enter the number of the native VLAN on the remote network (such as 100) in the Native VLAN ID text box.

Note By default, a VLAN is not enabled on the FlexConnect access point. When FlexConnect is enabled, the access point inherits the VLAN ID associated to the WLAN. This configuration is saved in the access point and received after the successful join response. By default, the native VLAN is 1. One native VLAN must be configured per FlexConnect access point in a VLAN-enabled domain. Otherwise, the access point cannot send and receive packets to and from the controller. When the client is assigned a VLAN from the RADIUS server, that VLAN is associated to the locally switched WLAN.

Step 9 Click the **Apply/Schedule** tab to save your changes.

Step 10 The Locally Switched VLANs section shows which WLANs are locally switched and provides their VLAN identifier. Click the **Edit** link to change the number of VLANs from which a client IP address is obtained. You are then redirected to a page where you can save the VLAN identifier changes.

Step 11 Click **Save** to save your changes.

Step 12 Repeat this procedure for any additional access points that need to be configured for FlexConnect at the remote site.

Connecting Client Devices to the WLANs

Follow the instructions for your client device to create profiles that connect to the WLANs you created in the "Configuring the Controller for FlexConnect" section on page 12-6.

In our example, you create three profiles on the client:

1. To connect to the "employee" WLAN, you create a client profile that uses WPA/WPA2 with PEAP-MSCHAPV2 authentication. When the client becomes authenticated, it gets an IP address from the management VLAN of the controller.
2. To connect to the "employee-local" WLAN, you create a client profile that uses WPA/WPA2 authentication. When the client becomes authenticated, it gets an IP address from VLAN 101 on the local switch.
3. To connect to the "guest-central" WLAN, you create a profile that uses open authentication. When the client becomes authenticated, it gets an IP address from VLAN 101 on the network local to the access point. After the client connects, the local user types any HTTP address in the web browser. You are automatically directed to the controller to complete the web-authentication process. When the web login page appears, enter the username and password.

To see if data traffic of the client is being locally or centrally switched, choose **Monitor > Devices > Clients**.

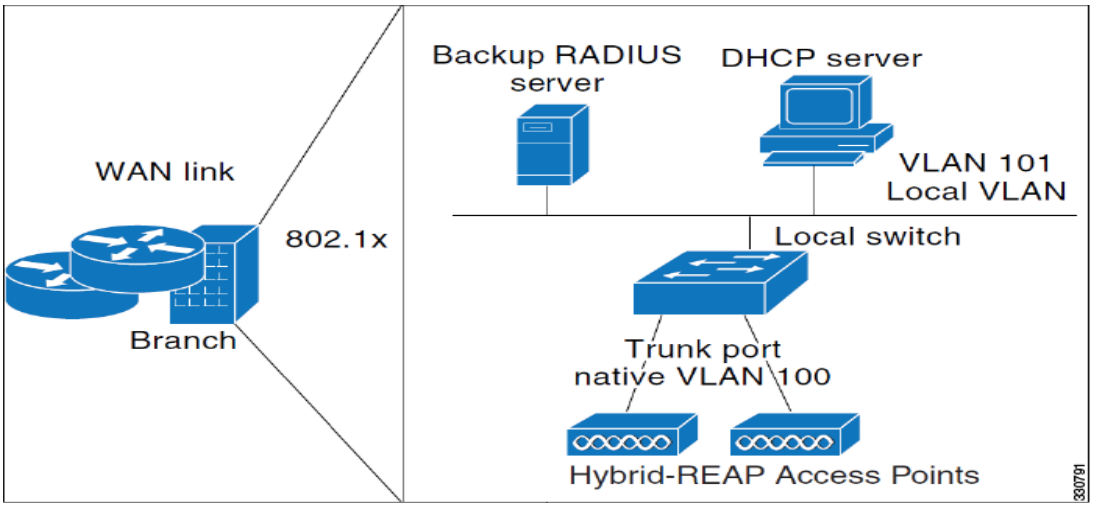
FlexConnect Access Point Groups

FlexConnect enables you to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. There is no deployment restriction on the number of FlexConnect access points per location, but you can organize and group the access points per floor and limit them per building, because it is likely the branch offices share the same configuration.

By forming access point groups with similar configurations, a procedure such as CCKM fast roaming can be processed more quickly than going through the controller individually. For example, to activate CCKM fast roaming, the FlexConnect access points must know the CCKM cache for all clients that could associate. If you have a controller with 300 access points and 1000 clients that can potentially connect, it is quicker and more practical to process and send the CCKM cache for the FlexConnect group rather than for all 1000 clients. One particular FlexConnect group could focus on a branch office with a small number of access points so that clients in the branch office could only connect to and roam between those few access points. With the established group, features such as CCKM cache and backup RADIUS are configured for the entire FlexConnect group rather than being configured in each access point.

All of the FlexConnect access points in a group share the same WLAN, backup RADIUS server, CCKM, and local authentication configuration information. This feature is helpful if you have multiple FlexConnect access points in a remote office or on the floor of a building and you want to configure them all at once. For example, you can configure a backup RADIUS server for a FlexConnect group rather than having to configure the same server on each access point. Figure 12-2 illustrates a typical FlexConnect group deployment with a backup RADIUS server in the branch office.

Figure 12-2 FlexConnect Group Deployment



This section contains the following topics:

- FlexConnect Groups and Backup RADIUS Servers, page 12-10
- FlexConnect Groups and CCKM, page 12-11
- FlexConnect Groups and Local Authentication, page 12-11
- Configuring FlexConnect Groups, page 12-11
- Auditing a FlexConnect Group, page 12-13

FlexConnect Groups and Backup RADIUS Servers

You can configure the controller to allow a FlexConnect access point in standalone mode to perform full 802.1x authentication to a backup RADIUS server. You can configure a primary RADIUS server or both a primary and secondary RADIUS server.

FlexConnect Groups and CCKM

FlexConnect groups are required for CCKM fast roaming to work with FlexConnect access points. CCKM fast roaming is achieved by caching a derivative of the master key from a full EAP authentication so that a simple and secure key exchange can occur when a wireless client roams to a different access point. This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one access point to another. The FlexConnect access points need to obtain the CCKM cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller. If, for example, you have a controller with 300 access points and 100 clients that might associate, sending the CCKM cache for all 100 clients is not practical. If you create a FlexConnect group comprising a limited number of access points (for example, you create a group for four access points in a remote office), the clients roam only among those four access points, and the CCKM cache is distributed among those four access points only when the clients associate to one of them.

Note CCKM fast roaming among FlexConnect and non-FlexConnect access points is not supported.

FlexConnect Groups and Local Authentication

You can configure the controller to allow a FlexConnect access point in standalone mode to perform LEAP or EAP-FAST authentication for up to 20 statically configured users. The controller sends the static list of usernames and passwords to each FlexConnect access point when it joins the controller. Each access point in the group authenticates only its own associated clients.

This feature is ideal for customers who are migrating from an autonomous access point network to a lightweight FlexConnect access point network and are not interested in maintaining a large user database nor adding another hardware device to replace the RADIUS server functionality available in the autonomous access point.

Note This feature can be used in conjunction with the FlexConnect backup RADIUS server feature. If a FlexConnect group is configured with both a backup RADIUS server and local authentication, the FlexConnect access point always attempts to authenticate clients using the primary backup RADIUS server first, followed by the secondary backup RADIUS server (if the primary is not reachable), and finally the FlexConnect access point itself (if the primary and secondary are not reachable).

Configuring FlexConnect Groups

To configure FlexConnect groups, follow these steps. If you want to apply a FlexConnect template to multiple controllers, see the template instructions in the "Configuring FlexConnect AP Groups Templates" section on page 10-41.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose a specific controller by clicking the desired IP address.

Step 3 From the left sidebar menu choose **FlexConnect > FlexConnect AP Groups**. The established FlexConnect AP groups appear.

Step 4 The Group Name column shows the group names assigned to the FlexConnect access point groups. If you want to add an additional group, choose **Add FlexConnect AP Group** from the Select a command drop-down list.

or

To make modifications to an existing template, click a template in the Template Name column. The General tab of the FlexConnect AP Groups Template page appears.

Note To delete a group name, click the group name you want to remove and choose **Delete FlexConnect AP Group** from the Select a command drop-down list.

The Template Name field shows the group name assigned to the FlexConnect access point group.

Step 5 Choose the primary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, the NCS-configured RADIUS server does not apply.

Note You must configure the RADIUS server configuration on the controller before you apply FlexConnect RADIUS server configuration from the NCS.

Step 6 Choose the secondary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, the NCS-configured RADIUS server does not apply.

Step 7 If you want to add an access point to the group, click the **FlexConnect AP** tab.

Step 8 An access point Ethernet MAC address cannot exist in more than one FlexConnect group on the same controller. If more than one group is applied to the same controller, select the **Ethernet MAC** check box to unselect an access point from one of the groups. You should save this change or apply it to controllers.

Step 9 If you want to enable local authentication for a FlexConnect group, click the **FlexConnect Configuration** tab. The FlexConnect Configuration tab appears.

Note Make sure that the Primary RADIUS Server and Secondary RADIUS Server parameters are set to **None** on the General tab.

Step 10 Select the **FlexConnect Local Authentication** check box to enable local authentication for this FlexConnect group. The default value is unselected.

Note When you attempt to use this feature, a warning message indicates that it is a licensed feature.

Step 11 To allow a FlexConnect access point to authenticate clients using LEAP, select the **LEAP** check box. Otherwise, to allow a FlexConnect access point to authenticate clients using EAP-FAST, select the **EAP-FAST** check box.

Step 12 Perform one of the following, depending on how you want protected access credentials (PACs) to be provisioned:

- To use manual PAC provisioning, enter the key used to encrypt and decrypt PACs in the EAP-FAST Key text box. The key must be 32 hexadecimal characters.
- To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select the **Auto Key Generation** check box.

Step 13 In the EAP-FAST Authority ID text box, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.

Step 14 In the EAP-FAST Authority Info text box, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.

Step 15 In the EAP-FAST Pac Timeout text box, specify a PAC timeout value by entering the number of seconds for the PAC to remain viable in the edit box. The valid range is 2 to 4095 seconds.

Note To verify that an individual access point belongs to a FlexConnect group, click the **Users configured in the group** link. It advances you to the FlexConnect AP Group page, which shows the names of the groups and the access points that belong in it.

Auditing a FlexConnect Group

If the FlexConnect configuration changes over a period of time either on the NCS or the controller, you can audit the configuration. The changes are visible on subsequent screens. You can choose to synchronize the configuration by refreshing the NCS or the controller.

CHAPTER 13

Alarm and Event Dictionary

This chapter describes the event and alarm notifications that the wireless LAN controller, access points, and location appliances can receive. It also identifies specific actions the administrator can take to address these alarms and events.

It describes the event and alarm notifications that the wireless LAN controller, access points, and location appliances can receive. In addition, specific actions an administrator can do to address these alarms and events are described.

Note Not all traps which are seen on the WLC graphical user interface are supported by the Cisco NCS.

This chapter contains the following sections:

- Unsupported Traps, page 13-165

Notification Format

For each alarm and event notification, the following information is provided (see Table 13-1).

Table 13-1 Trap Notification Format

Field	NCS Message
MIB Name	The MIB Name is the name of the notification as defined in the management information base (MIB). In some cases, if the event is specific only to the NMS, this field is not relevant. You can define multiple events in the NCS from the same trap based on the values of the variables present in the trap. In such cases, multiple subentries appear with the same MIB Name. In addition, this field displays the value of the variable that caused the NCS to generate this event.
Alarm Condition	This field displays the condition for which the trap was generated.
NCS Message	The NCS Message is a text string that reflects the message displayed in the NCS alarm or event browser associated with this event. Numbers such as "{0}" reflect internal NCS variables that typically are retrieved from variables in the trap. However, the order of the variables as they appear in the trap cannot be derived from the numbers.
Symptoms	This field displays the symptoms associated with this event.
Severity	This field displays the severity assigned to this event in the NCS.
Category	This field displays the category of the trap.
Probable Causes	This field lists the probable causes of the notification.
Recommended Actions	This field lists any actions recommended for the administrator managing the wireless network.

Traps Added in Release 2.0

The following traps were added to WCS Release 2.0:

- AP_BIG_NAV_DOS_ATTACK, page 13-5
- AP_CONTAINED_AS_ROGUE, page 13-5
- AP_HAS_NO_RADIOS, page 13-5
- AP_MAX_ROGUE_COUNT_CLEAR, page 13-6
- AP_MAX_ROGUE_COUNT_EXCEEDED, page 13-6
- AUTHENTICATION_FAILURE (From MIB-II standard), page 13-6
- BSN_AUTHENTICATION_FAILURE, page 13-7
- IPSEC_IKE_NEG_FAILURE, page 13-7
- IPSEC_INVALID_COOKIE, page 13-7
- LINK_DOWN (FROM MIB-II STANDARD), page 13-8
- LINK_UP (FROM MIB-II STANDARD), page 13-8

AP_BIG_NAV_DOS_ATTACK

MIB Name	bsnApBigNavDosAttack.
Alarm Condition	AP big nav DOS attack.
NCS Message	The AP "{0}" with protocol "{1}" receives a message with a large NAV field and all traffic on the channel is suspended. This is most likely a malicious denial of service attack.
Symptoms	The system detected a possible denial of service attack and suspended all traffic to the affected channel.
Severity	Critical.
Category	Security
Probable Causes	A malicious denial of service attack is underway.
Recommended Actions	Identify the source of the attack in the network and take the appropriate action immediately.

AP_CONTAINED_AS_ROGUE

MIB Name	bsnAPContainedAsARogue.
Alarm Condition	AP contained as rogue.
NCS Message	AP "{0}" with protocol "{1}" on Switch "{2}" is contained as a Rogue preventing service.
Symptoms	An access point is reporting that it is being contained as a rogue.
Severity	Critical.
Category	Access Point.
Probable Causes	Another system is containing this access point.
Recommended Actions	Identify the system containing this access point. You might need to use a wireless sniffer.

AP_HAS_NO_RADIOS

MIB Name	bsnApHasNoRadioCards.
Alarm Condition	AP has no radios.
NCS Message	AP "{0}" on Controller "{1}" has no Radio cards.
Symptoms	An access point is reporting that it has no radio cards.
Severity	Critical.
Category	Access Point.
Probable Causes	Manufacturing fault or damage to the system during shipping.
Recommended Actions	Call customer support.

AP_MAX_ROGUE_COUNT_CLEAR

MIB Name	bsnApMaxRogueCountClear.
Alarm Condition	AP maximum rogue count cleared.
NCS Message	Fake AP or other attack on AP with MAC address "{0}" associated with Switch "{2}" is cleared now. Rogue AP count is within the threshold of "{1}'."
Symptoms	The number of rogues detected by a switch (controller) is within acceptable limits.
Severity	Clear.
Category	Rogue AP
Probable Causes	None.
Recommended Actions	None.

AP_MAX_ROGUE_COUNT_EXCEEDED

MIB Name	bsnApMaxRogueCountExceeded.
Alarm Condition	AP maximum rogue count exceeded.
NCS Message	Fake AP or other attack might be in progress. Rogue AP count on AP with MAC address "{0}" associated with Switch "{2}" has exceeded the severity warning threshold of "{1}."
Symptoms	The number of rogues detected by a switch (controller) exceeds the internal threshold.
Severity	Critical.
Category	Rogue AP
Probable Causes	• There might be too many rogue access points in the network. • A fake access point attack might be in progress.
Recommended Actions	Identify the source of the rogue access points.

AUTHENTICATION_FAILURE (From MIB-II standard)

MIB Name	AuthenticationFailure.
Alarm Condition	Authentication failure reported by controller.
NCS Message	Switch "{0}". Authentication failure reported.
Symptoms	There was an SNMP authentication failure on the switch (controller).
Severity	Minor.
Category	Security
Probable Causes	An incorrect community string is in use by a management application.
Recommended Actions	Identify the source of the incorrect community string and correct the string within the management application.

BSN_AUTHENTICATION_FAILURE

MIB Name	bsnAuthenticationFailure.
Alarm Condition	Client authentication failure.
NCS Message	Switch "{0}." User authentication from Switch "{0}" failed for username "{1}" and user type "{2}."
Symptoms	A user authentication failure is reported for a local management user or a MAC filter is configured on the controller.
Severity	Minor.
Category	Clients
Probable Causes	Incorrect login attempt by an admin user from the controller command-line interface or controller graphical user interface, or a client accessing the WLAN system.
Recommended Actions	If the user has forgotten the password, the superuser might need to reset it.

IPSEC_IKE_NEG_FAILURE

MIB Name	bsnIpsecIkeNegFailure.
Alarm Condition	IPsec IKE negotiation failure.
NCS Message	IPsec IKE Negotiation failure from remote IP address "{0}."
Symptoms	Unable to establish an IPsec tunnel between a client and a WLAN appliance.
Severity	Minor.
Category	Security
Probable Causes	Configuration mismatch.
Recommended Actions	Validate configuration, verify that authentication credentials match (preshared keys or certificates); and verify that encryption algorithms and strengths match.

IPSEC_INVALID_COOKIE

MIB Name	bsnIpsecInvalidCookieTrap.
Alarm Condition	IPsec invalid cookie.
NCS Message	IPsec Invalid cookie from remote IP address "{0}."
Symptoms	Cannot successfully negotiate an IPsec session.
Severity	Minor.
Category	Security
Probable Causes	Synchronization problem. The client believes a tunnel exists while the WLAN appliance does not. This problem often happens when the IPsec client does not detect a disassociation event.
Recommended Actions	Reset the IPsec client and then restart tunnel establishment.

LINK_DOWN (FROM MIB-II STANDARD)

MIB Name	linkDown.
Alarm Condition	Interface state change.
NCS Message	Port "{0}" is down on Switch "{1}."
Symptoms	The physical link on one of the switch (controller) ports is down.
Severity	Critical.
Category	Controller.
Probable Causes	• An access point or a port was manually disconnected from the network. • A port failure.
Recommended Actions	Troubleshoot physical network connectivity to the affected port.

LINK_UP (FROM MIB-II STANDARD)

MIB Name	linkUp.
Alarm Condition	Interface state change.
NCS Message	Port "{0}" is up on Switch "{1}."
Symptoms	The physical link is up on a switch (controller) port.
Severity	Clear.
Category	Controller.
Probable Causes	A physical link to the switch (controller) is restored.
Recommended Actions	None.

LRAD_ASSOCIATED

MIB Name	bsnAPAssociated.
Alarm Condition	AP associated with controller.
NCS Message	AP "{0}" associated with Switch "{2}" on Port number "{1}."
Symptoms	An access point has associated with a switch (controller).
Severity	Clear.
Category	Access Point.
Probable Causes	• A new access point has joined the network. • An access point has associated with a standby switch (controller) due to a failover. • An access point rebooted and reassociated with a switch (controller).
Recommended Actions	Recycle the power and reset the software.

LRAD_DISASSOCIATED

MIB Name	bsnAPDisassociated.
Alarm Condition	AP disassociated from controller.
NCS Message	AP "{0}" disassociated from Switch "{1}."
Symptoms	The switch (controller) is no longer detecting an access point.
Severity	Critical.
Category	Access Point.
Probable Causes	• A failure in the access point. • An access point is no longer on the network.
Recommended Actions	Check if the access point is powered up and has network connectivity to the switch (controller).

LRADIF_COVERAGE_PROFILE_PASSED

MIB Name	bsnAPCoverageProfileUpdatedToPass.
Alarm Condition	Radio coverage threshold violation.
NCS Message	AP "{0},” interface "{1}." Coverage changed to acceptable.
Symptoms	A radio interface that was reporting coverage profile failure has reverted to an acceptable level.
Severity	Clear.
Category	Coverage Hole.
Probable Causes	The number of clients on this radio interface with suboptimal performance has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_CURRENT_CHANNEL_CHANGED

MIB Name	bsnAPCurrentChannelChanged.
Alarm Condition	Radio current channel changed.
NCS Message	AP "{0},” interface "{1}." Channel changed to "{2}." Interference Energy before update was "{3}" and after update is "{4}."
Symptoms	The current channel assigned to a radio interface has automatically changed.
Severity	Informational.
Category	Access Point.
Probable Causes	Possible interference on a channel has caused the radio management software on the controller to change the channel.
Recommended Actions	None.

LRADIF_CURRENT_TXPOWER_CHANGED

MIB Name	bsnAPCurrentTxPowerChanged.
Alarm Condition	Radio transmit power level changed.
NCS Message	AP "{0},” interface "{1}." Transmit Power Level changed to "{2}."
Symptoms	The power level has automatically changed on a radio interface.
Severity	Informational.
Category	Access Point.
Probable Causes	The radio management software on the controller has modified the power level for optimal performance.
Recommended Actions	None.

LRADIF_DOWN

MIB Name	bsnAPIfDown.
Alarm Condition	Radio administratively up and operationally down.
NCS Message	AP "{0},” interface "{1}" is down.
Symptoms	A radio interface is out of service.
Severity	Critical if not disabled, otherwise Informational.
Category	Access Point.
Probable Causes	• A radio interface has failed. • An administrator has disabled a radio interface. • An access point has failed and is no longer detected by the controller.
Recommended Actions	If the access point is not administratively disabled, call customer support.

LRADIF_INTERFERENCE_PROFILE_FAILED

MIB Name	bsnAPInterferenceProfileFailed.
Alarm Condition	Radio interference threshold violation.
NCS Message	AP "{0},” interface "{1}.” Interference threshold violated.
Symptoms	The interference detected on one or more channels is violated.
Severity	Minor.
Category	Access Points

Probable Causes	There are other 802.11 devices in the same band that are causing interference on channels used by this system.
Recommended Actions	• If the interference threshold is configured to be too low, you might need to readjust it to a more optimum value. • Investigate interference sources such as other 802.11 devices in the vicinity of this radio interface. A possible workaround is adding one or more access points to distribute the current load or slightly increasing the threshold of the access point which is displaying this message. To perform this workaround, follow the steps below: 1. Choose **Configure > Controllers**. 2. Click any IP address in that column of the All Controllers page. 3. From the left sidebar menu, choose **802.11a/n** or **802.11b/g/n** and then **RRM Thresholds**. 4. Adjust the Interference Threshold (%) in the Other Thresholds section.

LRADIF_INTERFERENCE_PROFILE_PASSED

MIB Name	bsnAPInterferenceProfileUpdatedToPass.
Alarm Condition	Radio interference threshold violation.
NCS Message	AP "{0},” interface "{1}." Interference changed to acceptable.
Symptoms	A radio interface reporting interference profile failure has reverted to an acceptable level.
Severity	Clear.
Category	Access Point.
Probable Causes	The interference on this radio interface has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_LOAD_PROFILE_FAILED

MIB Name	bsnAPLoadProfileFailed.
Alarm Condition	Radio load threshold violation.
NCS Message	AP "{0},” interface "{1}." Load threshold violated.
Symptoms	A radio interface of an access point is reporting that the client load has crossed a configured threshold.
Severity	Minor.
Category	Access Point.
Probable Causes	There are too many clients associated with this radio interface.
Recommended Actions	• Verify the client count on this radio interface. If the threshold for this trap is too low, you may need to readjust it. • Add new capacity to the physical location if the client count is a frequent issue on this radio.

LRADIF_LOAD_PROFILE_PASSED

MIB Name	bsnAPLoadProfileUpdatedToPass.
Alarm Condition	Radio load threshold violation.
NCS Message	AP "{0}," interface "{1}." Load changed to acceptable.
Symptoms	A radio interface that was reporting load profile failure has reverted to an acceptable level.
Severity	Clear.
Category	Access Point.
Probable Causes	The load on this radio interface has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_NOISE_PROFILE_FAILED

MIB Name	bsnAPNoiseProfileFailed.
Alarm Condition	Radio noise threshold violation.
NCS Message	AP "{0}," interface "{1}." Noise threshold violated.
Symptoms	The monitored noise level on this radio has crossed the configured threshold.
Severity	Minor.
Category	Access Point.
Probable Causes	Noise sources that adversely affect the frequencies on which the radio interface operates.
Recommended Actions	• If the noise threshold is too low, you may need to readjust it to a more optimal value. • Investigate noise sources in the vicinity of the radio interface (for example, a microwave oven).

LRADIF_NOISE_PROFILE_PASSED

MIB Name	bsnAPNoiseProfileUpdatedToPass.
Alarm Condition	Radio noise threshold violation.
NCS Message	AP "{0}," interface "{1}." Noise changed to acceptable.
Symptoms	A radio interface that was reporting noise profile failure has reverted to an acceptable level.
Severity	Clear.
Category	Access Point.
Probable Causes	The noise on this radio interface has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_UP

MIB Name	bsnAPIfUp.
Alarm Condition	Radio administratively up and operationally down.
NCS Message	AP "{0}," interface "{1}" is up.
Symptoms	A radio interface is up.
Severity	Clear.
Category	Access Point.
Probable Causes	• An administrator has enabled a radio interface. • An access point has turned on. • A new access point has joined the network.
Recommended Actions	None.

MAX_ROGUE_COUNT_CLEAR

MIB Name	bsnMaxRogueCountClear.
Alarm Condition	AP maximum rogue count cleared.
NCS Message	Fake AP or other attack is cleared now. Rogue AP count on system "{0}" is within the threshold of "{1}."
Symptoms	The number of rogues detected by a controller is within acceptable limits.
Severity	Clear.
Category	Rogue APs
Probable Causes	N/A.
Recommended Actions	None.

MAX_ROGUE_COUNT_EXCEEDED

MIB Name	bsnMaxRogueCountExceeded.
Alarm Condition	Maximum rogue count exceeded.
NCS Message	Fake AP or other attack might be in progress. Rogue AP count on system "{0}" has exceeded the severity warning threshold of "{1}."
Symptoms	The number of rogues detected by a controller exceeds the internal threshold.
Severity	Critical.
Category	Security
Probable Causes	• There are too many rogue access points in the network. • A fake access point attack is in progress.
Recommended Actions	Identify the source of the rogue access points.

MULTIPLE_USERS

MIB Name	multipleUsersTrap.
Alarm Condition	Multiple users.
NCS Message	Switch "{0}." Multiple users logged in.
Symptoms	Multiple users with the same login ID are logged in through the command-line interface.
Severity	Informational.
Category	Controller
Probable Causes	The same user has logged in multiple times through the command-line interface.
Recommended Actions	Verify that the expected login sessions for the same user is valid.

NETWORK_DISABLED

MIB Name	bsnNetworkStateChanged (bsnNetworkState set to disabled).
Alarm Condition	Network disabled
NCS Message	Global "{1}" network status disabled on Switch with IP Address "{0}."
Symptoms	An administrator has disabled the global network for 802.11a/n and 802.11b/g/n.
Severity	Informational.
Category	Controller
Probable Causes	Administrative command.
Recommended Actions	None.

NO_ACTIVITY_FOR_ROGUE_AP

MIB Name	This is a NCS-only event generated when no rogue activity is seen for a specific duration.
Alarm Condition	No activity for Rogue AP.
NCS Message	Rogue AP "{0}" is cleared explicitly. It is not detected anymore.
Symptoms	A rogue access point is cleared from the management system due to inactivity.
Severity	Informational.
Category	Rogue APs
Probable Causes	A rogue access point is not located on any managed controller for a specified duration.
Recommended Actions	None.

POE_CONTROLLER_FAILURE

MIB Name	bsnPOEControllerFailure.
Alarm Condition	PoE Controller Failure.
NCS Message	The POE controller has failed on the Switch "{0}."
Symptom	A failure in the Power Over Ethernet (POE) unit is detected.
Severity	Critical.
Category	Controller
Probable Causes	The power of the Ethernet unit has failed.
Recommended Actions	Call customer support. The unit might need to be repaired.

RADIO_ADMIN_UP_OPER_DOWN

MIB Name	bsnAPRadioCardRxFailure
Alarm Condition	Radio administratively up and operationally down.
NCS Message	{1} interface of AP {0} is down: Controller {2}
Symptom	None.
Severity	Critical
Category	Access Point
Probable Causes	None.
Recommended Actions	None.

RADIOS_EXCEEDED

MIB Name	bsnRadiosExceedLicenseCount.
Alarm Condition	Radios exceeded.
NCS Message	The Radios associated with Switch "{0}" exceeded license count "{1}." The current number of radios on this switch is "{2}."
Symptoms	The number of supported radios for a switch (controller) has exceeded the licensing limit.
Severity	Major.
Category	Controller
Probable Causes	The number of access points associated with the switch (controller) has exceeded the licensing limits.
Recommended Actions	Upgrade the license for the switch (controller) to support a higher number of access points.

RADIUS_SERVERS_FAILED

MIB Name	bsnRADIUSServerNotResponding.
Alarm Condition	RADIUS servers failure.
NCS Message	Switch "{0}." RADIUS server(s) are not responding to authentication requests.
Symptoms	The switch (controller) is unable to reach any RADIUS server for authentication.
Severity	Critical.
Category	Controller
Probable Causes	Network connectivity to the RADIUS server is lost or the RADIUS server is down.
Recommended Actions	Verify the status of all configured RADIUS servers and their network connectivity.

ROGUE_ADHOC_DETECTED

MIB Name	bsnRogueAPDetected.
Alarm Condition	Adhoc Rogue detected.
NCS Message	Rogue Adhoc "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Symptoms	A rogue adhoc was detected by the system.
Severity	Minor if not on wired network, critical if on wired network.
Category	Adhoc Rogue.
Probable Causes	• An illegal access point or adhoc has been connected to the network. • A known internal or external adhoc unknown to this system has been detected as rogue.
Recommended Actions	• Verify the nature of the adhoc point by tracing it through the MAC address/SSID or by using location features to locate it physically. • "If adhoc is a known internal or external adhoc, acknowledge it or mark it as a known adhoc. Consider adding it to the known access point template within the NCS. • If the adhoc is deemed to be a security threat, the rogue can be contained using the management interface.

ROGUE_ADHOC_ON_NETWORK

MIB Name	bsnRogueAPDetectedOnWiredNetwork
Alarm Condition	None.
NCS Message	Rogue ADHOC "{0}" is on wired network.
Symptoms	A rogue adhoc is found to be reachable through the wired network
Severity	Critical
Category	Switch
Probable Causes	• An illegal adhoc was detected to be reachable through the wired network. As a result its severity is escalated to critical
Recommended Actions	• Determine if this is a known or valid adhoc in the system. If so, place it in the known adhoc list. • Contain the rogue using the system to prevent anyone from accessing it until the adhoc has been traced down using location or other features.

ROGUE_AP_DETECTED

MIB Name	bsnRogueAPDetected.
Alarm Condition	ROGUE_AP_DETECTED
NCS Message	Rogue AP or ad hoc rogue "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}."
Symptoms	The system has detected a rogue access point.
Severity	Minor if not on a wired network; Critical if on a wired network.
Category	Rogue APs
Probable Causes	• An illegal access point is connected to the network. • A known internal or external access point unknown to this system is detected as rogue.
Recommended Actions	• Verify the nature of the rogue access point by tracing it using its MAC address or the SSID, or by using location features to locate it physically. • If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within the NCS. • If the access point is deemed to be a severity threat, contain it using the management interface.

ROGUE_AP_ON_NETWORK

MIB Name	bsnRogueAPDetectedOnWiredNetwork
Alarm Condition	ROGUE_AP_ON_NETWORK
NCS Message	Rogue AP or ad hoc rogue "{0}" is on the wired network.
Symptoms	A rogue access point is found reachable through the wired network.
Severity	Critical.
Category	Rogue AP
Probable Causes	An illegal access point was detected as reachable through the wired network.
Recommended Actions	• Determine if this is a known or valid access point in the system. If it is valid, place it in the known access point list. • Contain the rogue. Prevent anyone from accessing it until the access point has been traced down using location or other features.

ROGUE_AP_REMOVED

MIB Name	bsnRogueAPRemoved.
Alarm Condition	ROGUE_AP_REMOVED
NCS Message	Rogue AP or ad hoc rogue "{0}" is removed; it was detected as Rogue AP by AP "{1}" Radio type "{2}."
Symptoms	The system is no longer detecting a rogue access point.
Severity	Clear
Category	Rogue APs
Probable Causes	A rogue access point has powered off or moved away and therefore the system no longer detects it.
Recommended Actions	None.

RRM_DOT11_A_GROUPING_DONE

MIB Name	bsnRrmDot11aGroupingDone.
Alarm Condition	RRM
NCS Message	RRM 802.11a/n grouping done; the MAC address of the new group leader is "{0}."
Symptoms	The radio resource module is finished grouping for the A band, and a new group leader is chosen.
Severity	Informational.
Category	RRM
Probable Causes	The older RRM group leader might have gone down.
Recommended Actions	None.

RRM_DOT11_B_GROUPING_DONE

MIB Name	bsnRrmDot11bGroupingDone.
Alarm Condition	RRM
NCS Message	RRM 802.11b/g/n grouping done; the MAC address of the new group leader is "{0}."
Symptoms	The radio resource module finished its grouping for the B band and chose a new group leader.
Severity	Informational.
Category	RRM
Probable Causes	The older RRM group leader might have gone down.
Recommended Actions	None.

SENSED_TEMPERATURE_HIGH

MIB Name	bsnSensedTemperatureTooHigh.
Alarm Condition	Sensed temperature high.
NCS Message	The sensed temperature on the Switch "{0}" is too high. The current sensed temperature is "{1}."
Symptoms	The internal temperature of the system has crossed the configured thresholds.
Severity	Major.
Category	Controller
Probable Causes	• Fan failure. • Fault in the device.
Recommended Actions	• Verify the configured thresholds and increase the value if it is too low. • Call customer support.

SENSED_TEMPERATURE_LOW

MIB Name	bsnSensedTemperatureTooLow.
Alarm Condition	Sensed temperature low.
NCS Message	The sensed temperature on the Switch "{0}" is too low. The current sensed temperature is "{1}."
Symptoms	The internal temperature of the device is below the configured limit in the system.
Severity	Major.
Category	Controller
Probable Causes	• Operating environment. • Hardware fault.
Recommended Actions	• Verify the configured thresholds and ensure that the limit is appropriate. • Call customer support.

STATION_ASSOCIATE

MIB Name	bsnDot11StationAssociate.
Alarm Condition	Client associated to AP.
NCS Message	Client "{0}" is associated with AP "{1}," interface "{2}."
Symptoms	A client has associated with an access point.
Severity	Informational.
Category	Clients
Probable Causes	A client has associated with an access point.
Recommended Actions	None.

STATION_ASSOCIATE_FAIL

MIB Name	bsnDot11StationAssociateFail.
Alarm Condition	Client associated failure with AP.
NCS Message	Client "{0}" failed to associate with AP "{1}," interface "{2}." The reason code is "{3}."
Symptoms	A client station failed to associate with the system.
Severity	Informational.
Category	Clients
Probable Causes	The access point was busy.
Recommended Actions	Check whether the access point is busy and reporting load profile failures.

STATION_AUTHENTICATE

MIB Name	bsnDot11StationAssociate (bsnStationUserName is set).
Alarm Condition	Client authenticated.
NCS Message	Client "{0}" with username "{3}" is authenticated with AP "{1}," interface "{2}."
Symptoms	A client has successfully authenticated with the system.
Severity	Informational.
Category	Clients
Probable Causes	A client has successfully authenticated with the system.
Recommended Actions	None.

STATION_AUTHENTICATION_FAIL

MIB Name	bsnDot11StationAuthenticateFail.
Alarm Condition	Client authentication failure.
NCS Message	Client "{0}" has failed authenticating with AP "{1}," interface "{2}." The reason code is "{3}."
Symptoms	The system failed to authenticate a client.
Severity	Informational.
Category	Clients
Probable Causes	Failed client authentication.
Recommended Actions	Check client configuration and configured keys or passwords in the system.

STATION_BLACKLISTED

MIB Name	bsnDot11StationBlacklisted.
Alarm Condition	Client excluded.

NCS Message	Client "{0}" which was associated with AP "{1}," interface "{2}" is excluded. The reason code is "{3}."
Symptoms	A client is in the exclusion list and is not allowed to authenticate for a configured interval.
Severity	Minor.
Category	Security
Probable Causes	• Repeated authentication or association failures from the client station. • A client is attempting to use an IP address assigned to another device.
Recommended Actions	• Verify the configuration or the client along with its credentials. • Remove the client from the exclusion list by using the management interface if the client needs to be allowed back into the network.

STATION_DEAUTHENTICATE

MIB Name	bsnDot11StationDeauthenticate.
Alarm Condition	Client deauthenticated from AP.
NCS Message	Client "{0}" is deauthenticated from AP "{1}," interface "{2}" with reason code "{3}."
Symptoms	A client is no longer authenticated by the system.
Severity	Informational.
Category	Clients
Probable Causes	A client is no longer authenticated by the system.
Recommended Actions	None.

STATION_DISASSOCIATE

MIB Name	bsnDot11StationDisassociate.
Alarm Condition	Client disassociated from AP.
NCS Message	Client "{0}" is disassociated from AP "{1}," interface "{2}" with reason code "{3}."
Symptoms	A client has disassociated with an access point in the system.
Severity	Informational.
Category	Clients
Probable Causes	A station might disassociate due to various reasons such as inactivity timeout or a forced action from the management interface.
Recommended Actions	None.

STATION_WEP_KEY_DECRYPT_ERROR

MIB Name	bsnWepKeyDecryptError.
Alarm Condition	Client WEP key decryption error.
NCS Message	The WEP Key configured at the station might be wrong. Station MAC Address is "{0}," AP MAC is "{1}" and Slot ID is "{2}."
Symptoms	A client station seems to have the wrong WEP key.
Severity	Minor.
Category	Security
Probable Causes	A client has an incorrectly configured WEP key.
Recommended Actions	Identify the client and correct the WEP key configuration.

STATION_WPA_MIC_ERROR_COUNTER_ACTIVATED

MIB Name	bsnWpaMicErrorCounterActivated.
Alarm Condition	Client WPA MIC error counter activated.

NCS Message	The AP "{1}" received a WPA MIC error on protocol "{2}" from Station "{0}." Counter measures have been activated and traffic has been suspended for 60 seconds.
Symptoms	A client station has detected a WPA MIC error.
Severity	Critical.
Category	Security
Probable Causes	A possible hacking attempt is underway.
Recommended Actions	Identify the station that is the source of this threat.

SWITCH_DETECTED_DUPLICATE_IP

MIB Name	bsnDuplicateIpAddressReported.
Alarm Condition	Controller Detected Duplicate IP.
NCS Message	Switch "{0}" detected duplicate IP address "{0}" being used by machine with mac address "{1}."
Symptoms	The system has detected a duplicate IP address in the network that is assigned to the switch (controller).
Severity	Critical.
Category	Security
Probable Causes	Another device in the network is configured with the same IP address as that of the switch (controller).
Recommended Actions	Correct the misconfiguration of IP addresses in the network.

SWITCH_UP

MIB Name	This is a NCS-only event.
Alarm Condition	Controller up.
NCS Message	Switch "{0}" is reachable.
Symptoms	A switch (controller) is now reachable from the management station.
Severity	Clear.
Category	Switch
Probable Causes	A switch (controller) is reachable from the management station.
Recommended Actions	None.

TEMPERATURE_SENSOR_CLEAR

MIB Name	bsnTemperatureSensorClear.
Alarm Condition	Temperature sensor clear.
NCS Message	The temperature sensor is working now on the switch "{0}." The sensed temperature is "{1}."
Symptoms	The temperature sensor is operational.
Severity	Clear.
Category	Controller
Probable Causes	The system is detecting the temperature sensor to be operational now.
Recommended Actions	None.

TEMPERATURE_SENSOR_FAILURE

MIB Name	bsnTemperatureSensorFailure.
Alarm Condition	Temperature sensor failure

NCS Message	The temperature sensor failed on the Switch "{0}." Temperature is unknown.
Symptoms	The system is reporting that a temperature sensor has failed and the system is unable to report accurate temperature.
Severity	Major.
Category	Controller
Probable Causes	The temperature sensor has failed due to hardware failure.
Recommended Actions	Call customer support.

TOO_MANY_USER_UNSUCCESSFUL_LOGINS

MIB Name	bsnTooManyUnsuccessLoginAttempts.
Alarm Condition	Too many user unsuccessful logins.
NCS Message	User "{1}" with IP Address "{0}" has made too many unsuccessful login attempts.
Symptoms	A management user has made too many login attempts.
Severity	Critical.
Category	Security
Probable Causes	• An admin user has made too many login attempts. • A user attempted to break into the administration account of the management system.
Recommended Actions	• Identify the source of the login attempts and take the appropriate action. • Increase the value of the login attempt threshold if it is too low.

Traps Added in Release 2.1

The following traps were added for WCS Release 2.1:

ADHOC_ROGUE_AUTO_CONTAINED

MIB Name	bsnAdhocRogueAutoContained.
Alarm Condition	Adhoc Rogue auto contained.
NCS Message	Adhoc Rogue "{0}" was found and is auto contained as per WPS policy.
Symptoms	The system detected an ad hoc rogue and automatically contained it.
Severity	Major.
Category	Security
Probable Causes	The system detected an ad hoc rogue and automatically contained it as configured in the wireless prevention policy of the system.
Recommended Actions	Identify the ad hoc rogue through the location application and take the appropriate action.

ADHOC_ROGUE_AUTO_CONTAINED_CLEAR

MIB Name	bsnAdhocRogueAutoContained (bsnClearTrapVariable set to true).
Alarm Condition	Adhoc Rogue auto contained cleared.
NCS Message	Adhoc Rogue "{0}" was found and was auto contained. The alert state is clear now.
Symptoms	An ad hoc rogue that the system has detected earlier is now clear.
Severity	Clear.
Category	Security
Probable Causes	The system no longer detects an ad hoc rogue.
Recommended Actions	None.

NETWORK_ENABLED

MIB Name	bsnNetworkStateChanged (bsnNetworkState set to enabled).
Alarm Condition	Network enabled.
NCS Message	Global "{1}" network status enabled on Switch with IP Address "{0}."
Symptoms	An administrator has enabled the global network for 802.11a/n or 802.11b/g/n.
Severity	Informational.
Category	Controller
Probable Causes	Administrative command.
Recommended Actions	None.

ROGUE_AP_AUTO_CONTAINED

MIB Name	bsnRogueApAutoContained.
Alarm Condition	Rogue AP auto contained.

NCS Message	Rogue AP "{0}" is advertising our SSID and is auto contained as per WPS policy.
Symptoms	The system has automatically contained a rogue access point.
Severity	Major.
Category	Rogue APs
Probable Causes	The system detected an ad hoc rogue and automatically contained it as configured in the wireless prevention policy of the system.
Recommended Actions	• Track the location of the rogue and take the appropriate action. • If this is a known valid access point, clear the rogue from containment.

ROGUE_AP_AUTO_CONTAINED_CLEAR

MIB Name	bsnRogueApAutoContained (bsnClearTrapVariable set to true).
Alarm Condition	Rogue AP cleared.
NCS Message	Rogue AP "{0}" was advertising our SSID and was auto contained. The alert state is clear now.
Symptoms	The system has cleared a previously contained rogue.
Severity	Clear.
Category	Rogue APs
Probable Causes	The system has cleared a previously contained rogue.
Recommended Actions	None.

TRUSTED_AP_INVALID_ENCRYPTION

MIB Name	bsnTrustedApHasInvalidEncryption.
Alarm Condition	Trusted AP with invalid encryption.
NCS Message	Trusted AP "{0}" is invalid encryption. It is using "{1}" instead of "{2}." It is auto contained as per WPS policy.
Symptoms	The system automatically contained a trusted access point that has invalid encryption.
Severity	Major.
Category	Security
Probable Causes	The system automatically contained a trusted access point that violated the configured encryption policy.
Recommended Actions	Identify the trusted access point and take the appropriate action.

TRUSTED_AP_INVALID_ENCRYPTION_CLEAR

MIB Name	bsnTrustedApHasInvalidEncryption (bsnClearTrapVariable set to true).
Alarm Condition	Trusted AP with invalid encryption cleared.
NCS Message	Trusted AP "{0}" had invalid encryption. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
Severity	Clear.
Category	Security
Probable Causes	The trusted access point has now conformed to the configured encryption policy.
Recommended Actions	None.

TRUSTED_AP_INVALID_RADIO_POLICY

MIB Name	bsnTrustedApHasInvalidRadioPolicy.
Alarm Condition	Trusted AP with invalid radio policy.

NCS Message	Trusted AP "{0}" has invalid radio policy. It is using "{1}" instead of "{2}." It has been auto contained as per WPS policy.
Symptoms	The system has contained a trusted access point with an invalid radio policy.
Severity	Major.
Category	Security
Probable Causes	The system has contained a trusted access point connected to the wireless system for violating the configured radio policy.
Recommended Actions	Identify the trusted access point and take the appropriate action.

TRUSTED_AP_INVALID_RADIO_POLICY_CLEAR

MIB Name	bsnTrustedApHasInvalidRadioPolicy (bsnClearTrapVariable set to true).
Alarm Condition	Trusted AP with invalid radio policy cleared.
NCS Message	Trusted AP "{0}" had invalid radio policy. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
Severity	Clear.
Category	Security
Probable Causes	The trusted access point has now conformed to the configured encryption policy.
Recommended Actions	None.

TRUSTED_AP_INVALID_SSID

MIB Name	bsnTrustedApHasInvalidSsid.
Alarm Condition	Trusted AP with invalid SSID
NCS Message	Trusted AP "{0}" has invalid SSID. It was auto contained as per WPS policy.
Symptoms	The system has automatically contained a trusted access point for advertising an invalid SSID.
Severity	Major.
Category	Security
Probable Causes	The system has automatically contained a trusted access point for violating the configured SSID policy.
Recommended Actions	Identify the trusted access point and take the appropriate action.

TRUSTED_AP_INVALID_SSID_CLEAR

MIB Name	bsnTrustedApHasInvalidSsid (bsnClearTrapVariable set to true).
Alarm Condition	Trusted AP with invalid SSID clear.
NCS Message	Trusted AP "{0}" had invalid SSID. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
Severity	Clear.
Category	Security
Probable Causes	The trusted access point has now conformed to the configured policy.
Recommended Actions	None.

TRUSTED_AP_MISSING

MIB Name	bsnTrustedApIsMissing.
Alarm Condition	Trusted AP missing.
NCS Message	Trusted AP "{0}" is missing or has failed.

Symptoms	The wireless system no longer detects a trusted access point.
Severity	Major.
Category	Security
Probable Causes	A trusted access point has left the network or has failed.
Recommended Actions	Track down the trusted access point and take the appropriate action.

TRUSTED_AP_MISSING_CLEAR

MIB Name	bsnTrustedApIsMissing (bsnClearTrapVariable set to true).
Alarm Condition	Trusted AP missing clear.
NCS Message	Trusted AP "{0}" is missing or has failed. The alert state is clear now.
Symptoms	The system has found a trusted access point again.
Severity	Clear.
Category	Security
Probable Causes	The system has detected a previously missing trusted access point.
Recommended Actions	None.

Traps Added in Release 2.2

The following traps were added in WCS Release 2.2:

- AP_IMPERSONATION_DETECTED, page 13-33
- AP_RADIO_CARD_RX_FAILURE, page 13-33
- AP_RADIO_CARD_RX_FAILURE_CLEAR, page 13-33
- AP_RADIO_CARD_TX_FAILURE, page 13-34
- AP_RADIO_CARD_TX_FAILURE_CLEAR, page 13-34
- SIGNATURE_ATTACK_CLEARED, page 13-34
- SIGNATURE_ATTACK_DETECTED, page 13-34
- TRUSTED_AP_INVALID_PREAMBLE, page 13-35
- TRUSTED_AP_INVALID_PREAMBLE_CLEARED, page 13-35

AP_IMPERSONATION_DETECTED

MIB Name	bsnAPImpersonationDetected.
Alarm Condition	AP impersonation detected.
NCS Message	AP Impersonation with MAC "{0}" is detected by authenticated AP "{1}" on "{2}" radio and Slot ID "{3}."
Symptoms	A radio of an authenticated access point has heard from another access point whose MAC address neither matches that of a rogue nor is it an authenticated neighbor of the detecting access point.
Severity	Critical.
Category	Security
Probable Causes	A severity breach related to access point impersonation might be under way.
Recommended Actions	Track down the MAC address of the impersonating access point in the network and contain it.

AP_RADIO_CARD_RX_FAILURE

MIB Name	bsnAPRadioCardRxFailure.
Alarm Condition	AP impersonation detected.
NCS Message	Receiver failure detected on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio card is unable to receive data.
Severity	Critical.
Category	Security
Probable Causes	• A radio card is experiencing reception failure. • The antenna of the radio is disconnected.
Recommended Actions	• Check the antenna connection of the access point. • Call customer support.

AP_RADIO_CARD_RX_FAILURE_CLEAR

MIB Name	bsnAPRadioCardRxFailureClear.
Alarm Condition	Radiocard failure clear.
NCS Message	Receiver failure cleared on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio is no longer experiencing reception failure.
Severity	Clear.
Category	Access Point.
Probable Causes	A malfunction in the access point has been corrected.
Recommended Actions	None.

AP_RADIO_CARD_TX_FAILURE

MIB Name	bsnAPRadioCardTxFailure.
Alarm Condition	Radiocard failure.
NCS Message	Transmitter failure detected on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio card is unable to transmit.
Severity	Critical.
Category	Access Point.
Probable Causes	• A radio card is experiencing transmission failure. • The antenna of the radio might be disconnected.
Recommended Actions	• Check the antenna of the access point. • Call customer support.

AP_RADIO_CARD_TX_FAILURE_CLEAR

MIB Name	bsnAPRadioCardTxFailureClear.
Alarm Condition	NA
NCS Message	Transmitter failure cleared on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio is no longer experiencing transmission failure.
Severity	Clear.
Category	Access Point.
Probable Causes	A malfunction in the access point has been corrected.
Recommended Actions	None.

SIGNATURE_ATTACK_CLEARED

MIB Name	bsnSignatureAttackDetected (bsnClearTrapVariable is set to True).
Alarm Condition	Signature attack cleared.
NCS Message	Switch "{0}" is cleared from IDS signature attack. The wireless system is no longer detecting the intrusion.
Symptoms	The switch (controller) no longer detects a signature attack.
Severity	Clear.
Category	Security
Probable Causes	The signature attack that the system previously detected has stopped.
Recommended Actions	None.

SIGNATURE_ATTACK_DETECTED

MIB Name	bsnSignatureAttackDetected
Alarm Condition	Signature attack detected

NCS Message	IDS Signature attack detected on Switch "{0}." The Signature Type is "{1}," Signature Name is "{2}," and Signature description is "{3}."
Symptoms	The switch (controller) is detecting a signature attack. The switch (controller) has a list of signatures that it monitors. When it detects a signature, it provides the name of the signature attack in the alert it generates.
Severity	Critical.
Category	Security
Probable Causes	Someone is mounting a malevolent signature attack.
Recommended Actions	Track down the source of the signature attack in the wireless network and take the appropriate action.

TRUSTED_AP_INVALID_PREAMBLE

MIB Name	bsnTrustedApHasInvalidPreamble.
Alarm Condition	Trusted AP with invalid preamble.
NCS Message	Trusted AP "{0}" on Switch "{3}" has invalid preamble. It is using "{1}" instead of "{2}." It has been auto contained as per WPS policy.
Symptoms	The system has contained a trusted rogue access point for using an invalid preamble.
Severity	Major.
Category	Security
Probable Causes	The system has detected a possible severity breach because a rogue is transmitting an invalid preamble.
Recommended Actions	Locate the rogue access point using location features or the access point detecting it and take the appropriate actions.

TRUSTED_AP_INVALID_PREAMBLE_CLEARED

MIB Name	bsnTrustedApHasInvalidPreamble (bsnClearTrapVariable is set to true).
Alarm Condition	Trusted AP with invalid preamble cleared.
NCS Message	Trusted AP "{0}" on Switch "{3}" had invalid preamble. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
Severity	Clear.
Category	Security
Probable Causes	The system has cleared a previous alert about a trusted access point.
Recommended Actions	None.

Traps Added in Release 3.0

The following traps were added in WCS Release 3.0:

AP_FUNCTIONALITY_DISABLED

MIB Name	bsnAPFunctionalityDisabled.
Alarm Condition	AP functionality disabled.
NCS Message	AP functionality has been disabled for key "{0}," reason being "{1}" for feature-set "{2}."
Symptoms	The system sends this trap out when the controller disables access point functionality because the license key has expired.
Severity	Critical.
Category	Controller
Probable Causes	When the controller boots up, it checks whether the feature license key matches the software image of the controller. If it does not, the controller disables access point functionality.
Recommended Actions	Configure the correct license key on the controller and reboot it to restore access point functionality.

AP_IP_ADDRESS_FALLBACK

MIB Name	bsnAPIPAddressFallback.
Alarm Condition	AP IP fallback.
NCS Message	AP "{0}" with static-ip configured as "{2}" has fallen back to the working DHCP address "{1}."
Symptoms	This trap is sent out when an access point, with the configured static ip-address, fails to establish connection with the outside world and starts using DHCP as a fallback option.
Severity	Minor.
Category	Access Point.
Probable Causes	If the configured IP address on the access point is incorrect or obsolete, and if the AP Fallback option is enabled on the switch (controller), the access point starts using DHCP.
Recommended Actions	Reconfigure the static IP of the access point to the correct IP address if desired.

AP_REGULATORY_DOMAIN_MISMATCH

MIB Name	bsnAPRegulatoryDomainMismatch.
Alarm Condition	AP regulatory domain mismatch.
NCS Message	AP "{1}" is unable to associate. The Regulatory Domain configured on it "{3}" does not match the Controller "{0}" country code "{2}."
Symptoms	The system generates this trap when the regulatory domain of an access point does not match the country code configured on the controller. Due to the country code mismatch, the access point fails to associate with the controller.
Severity	Critical.
Category	Access Point.

Probable Causes	• If someone changes the country code configuration of the controller and some of the existing access points support a different country code, these access points fail to associate. • An access point on the network of a controller sends join requests to the controller, but the regulatory domain is outside the domain in which the controller is operating.
Recommended Actions	Either remove the access points that are not meant for inclusion in the domain of the controller or correct the country code setting of the controller.

RX_MULTICAST_QUEUE_FULL

MIB Name	bsnRxMulticastQueueFull.
Alarm Condition	CPU RX Multicast queue full.
NCS Message	CPU Receive Multicast Queue is full on Controller "{0}."
Symptoms	This trap indicates that the Receive Multicast queue of the CPU is full.
Severity	Critical.
Category	Controller
Probable Causes	An ARP storm.
Recommended Actions	None.

Traps Added in Release 3.1

The following traps were added in WCS Release 3.1:

AP_AUTHORIZATION_FAILURE

MIB Name	bsnAPAuthorizationFailure
Alarm Condition	AP Authorization Failure.
NCS Message	• Failed to authorize AP “{0}." Authorization entry does not exist in Controllers “{1}” AP Authorization List. • Failed to authorize AP “{0}." The authorization key of the AP does not match with SHA1 key in Controllers “{1}” AP Authorization List. • Failed to authorize AP “{0}." Controller “{1}” could not verify the Self Signed Certificate from the AP. • Failed to authorize AP “{0}." AP has a self signed certificate where as the Controllers “{1}” AP authorization list has Manufactured Installed Certificate for this AP.
Symptoms	An alert is generated when an access point fails to associate with a controller due to authorization issues.
Severity	Critical.
Category	Access Point.
Probable Causes	• The access point is not on the controller's access point authorization list. • The key entry in the controller's access point authorization list does not match the SHA1 key received from the access point. • The access point self-signed certificate is not valid. • The access point has a self-signed certificate and the access point authorization list of the controller (for the given access point) references a manufactured installed certificate.
Recommended Actions	• Add the access point to the authorization list of the controller. • Update the authorization key of the access point to match the access point key of the controller. • Check the accuracy of the self-signed certificate of the access point. • Check the certificate type of the access point in the access point authorization list of the controller.

HEARTBEAT_LOSS_TRAP

MIB Name	heartbeatLossTrap.
Alarm Condition	Heart beat loss.
NCS Message	Keepalive messages are lost between Master and Controller"{0}.”
Symptoms	This trap is generated when the controller loses connection with the Supervisor Switch (in which it is physically embedded) and the controller cannot hear the heartbeat (keepalives) from the Supervisor.
Severity	Major.
Category	Controller

Probable Causes	• Port on the WiSM controller could be down. • Loss of connection with the Supervisor Switch.
Recommended Actions	None.

INVALID_RADIO_INTERFACE

MIB Name	invalidRadioTrap.
Alarm Condition	Invalid radio interface.
NCS Message	Radio with MAC address “{0}” and protocol “{1}” that has joined controller “{2}” has invalid interface. The reason is “{3}.”
Symptoms	If a Cisco access point joins the network but has unsupported radios, the controller detects this and generates a trap. This symptom propogates an alert in the NCS.
Severity	Critical.
Category	Controller
Probable Causes	The radio hardware is not supported by the controller.
Recommended Actions	None.

RADAR_CLEARED

MIB Name	bsnRadarChannelCleared
Alarm Condition	NA
NCS Message	Radar has been cleared on channel "{1}" which was detected by AP base radio MAC "{0}" on radio 802.11a/n.
Symptoms	Trap is generated after the expiry of a non-occupancy period for a channel that previously generated a radar trap.
Severity	Clear.
Category	Access Point.
Probable Causes	Trap is cleared on a channel.
Recommended Actions	None.

RADAR_DETECTED

MIB Name	bsnRadarChannelDetected
Alarm Condition	NA
NCS Message	Radar has been detected on channel "{1}" by AP base radio MAC "{0}" on radio 802.11a/n.
Symptoms	This trap is generated when radar is detected on the channel on which an access point is currently operating.
Severity	Informational.
Category	Access Point.
Probable Causes	Radar is detected on a channel.
Recommended Actions	None.

RADIO_CORE_DUMP

MIB Name	radioCoreDumpTrap
Alarm Condition	Radio Core Dump.
NCS Message	Radio with MAC address “{0}” and protocol “{1}” has core dump on controller “{2}."
Symptoms	When a Cisco radio fails and a core dump occurs, the controller generates a trap and the NCS generates an event for this trap.
Severity	Informational.
Category	Access Point.
Probable Causes	Radio failure.
Recommended Actions	Capture the core dump file using the command-line interface of the controller and send to TAC support.

RADIO_INTERFACE_DOWN

MIB Name	bsnAPIfDown.
Alarm Condition	Radio Interface Down
NCS Message	Radio with MAC address “{0}” and protocol “{1}” is down. The reason is “{2}.”
Symptoms	When a radio interface is down, the NCS generates an alert. Reason for the radio outage is also noted.
Severity	Critical if not manually disabled. Informational if radio interface was manually disabled.
Category	Access Point.
Probable Causes	• The radio interface has failed. • The access point cannot draw enough power. • The maximum number of transmissions for the access point is reached. • The access point has lost connection with the controller heart beat. • The admin status of the access point admin is disabled. • The admin status of the radio is disabled.
Recommended Actions	None.

RADIO_INTERFACE_UP

MIB Name	bsnAPIfUp.
Alarm Condition	Radio interface up.
NCS Message	Radio with MAC address “{0}” and protocol “{1}” is up. The reason is “{2}.”
Symptoms	When a radio interface is operational again, the NCS clears the previous alert. Reason for the radio being up again is also noted.
Severity	Clear.

Category	Access Point.
Probable Causes	• Admin status of access point is enabled. • Admin status of radio is enabled. • Global network admin status is enabled.
Recommended Actions	None.

UNSUPPORTED_AP

MIB Name	unsupportedAPTrap.
Alarm Condition	Unsupported AP.
NCS Message	AP "{0}" tried to join controller "{1}" and failed. The controller does not support this kind of AP.
Symptoms	When unsupported access points try to join 40xx/410x controllers or 3500 controller with 64 MB flash, these controllers generate a trap, and the trap is propagated as an event in the NCS.
Severity	Informational.
Category	Access Point.
Probable Causes	Access point is not supported by the controller.
Recommended Actions	None.

Traps Added in Release 3.2

The following trap was added in WCS Release 3.2:

LOCATION_NOTIFY_TRAP

MIB Name	locationNotifyTrap.
Alarm Condition	Location notify.
NCS Message	Depending on the notification condition reported, the trap is sent out in an XML format and is reflected in the NCS with the following alert messages: • Absence of <Element> with MAC <macAddress>, last seen at <timestamp>. • <Element> with MAC <macAddress> is <In | Out> the Area <campus | building | floor | coverageArea>. • <Element> with MAC <macAddress> has moved beyond <specifiedDistance> ft. of marker <MarkerName>, located at a range of <foundDistance> ft. For detailed info on the XML format for the trap content, consult the *2700 Location Appliance Configuration Guide*.
Symptoms	A 2700 location appliance sends this trap out when the defined location notification conditions are met (such at element outside area, elements missing, and elements exceeded specified distance). The NCS uses this trap to display alarms about location notification conditions.
Severity	Minor (under the Location Notification dashboard).
Category	Context Aware Notifications
Probable Causes	The location notification conditions configured for a 2700 location appliance are met for certain elements on the network.
Recommended Actions	None.

Traps Added In Release 4.0

The following traps were added in WCS Release 4.0:

- GUEST_USER_REMOVED_TRAP, page 13-50

CISCO_LWAPP_MESH_POOR_SNR

MIB Name	ciscoLwappMeshPoorSNR
Alarm Condition	NA
NCS Message	Poor SNR.
Symptoms	SNR (signal-to-noise) ratio is important because high signal strength is not enough to ensure good receiver performance. The incoming signal must be stronger than any noise or interference that is present. For example, you can have high signal strength and still have poor wireless performance if there is strong interference or a high noise level.
Severity	Major.
Category	Mesh
Probable Causes	The link SNR fell below 12 db. The threshold level cannot be changed. If poor SNR is detected on the backhaul link for a child or parent, the trap is generated and contains SNR values and MAC addresses.
Recommended Actions	None.

CISCO_LWAPP_MESH_PARENT_CHANGE

MIB Name	ciscoLwappMeshParentChange
Alarm Condition	NA
NCS Message	Parent changed.
Symptoms	When the parent is lost, the child joins with another parent, and the child sends traps containing both old and new MAC addresses of the parent.
Severity	Informational
Category	Mesh
Probable Causes	The child moved to another parent.
Recommended Actions	None.

CISCO_LWAPP_MESH_CHILD_MOVED

MIB Name	ciscoLwappMeshChildMoved
Alarm Condition	Done.
NCS Message	Child moved.
Symptoms	When the parent access point detects a child being lost and communication is halted, the child lost trap is sent to the NCS, along with the child MAC address.

Severity	Informational
Category	Mesh
Probable Causes	The child moved from the parent.
Recommended Actions	None.

CISCO_LWAPP_MESH_CONSOLE_LOGIN

MIB Name	ciscoLwappMeshConsoleLogin
Alarm Condition	NA
NCS Message	Console login successful or failed.
Symptoms	The console port provides the ability for the customer to change the username and password to recover the stranded outdoor access point. To prevent any unauthorized user access to the access point, the NCS sends an alarm when someone tries to log in. This alarm is required to provide protection because the access point is physically vulnerable being located outdoors.
Severity	A login is of critical severity.
Category	Mesh
Probable Causes	You have successfully logged in to the access point console port or failed on three consecutive tries.
Recommended Actions	None.

CISCO_LWAPP_MESH_AUTHORIZATION_FAILURE

MIB Name	ciscoLwappMeshAuthorizationFailure
Alarm Condition	NA
NCS Message	Fails to authenticate with controller.
Symptoms	The NCS receives a trap from the controller. The trap contains the MAC addresses of those access points that failed authorization.
Severity	Minor.
Category	Mesh
Probable Causes	The access point tried to join the MESH but failed to authenticate because the MESH node MAC address was not on the MAC filter list.
Recommended Actions	None.

EXCESSIVE_ASSOCIATION

MIB Name	ciscoLwappMeshExcessiveAssociationFailure
Alarm Condition	NA
NCS Message	Excessive association failures.
Symptoms	This trap is raised after a failed-association-attempt exceeds the threshold (which is not user configurable). Association failures are cumulative of the total failures from different MAPs. The trap sent by the controller contains the MAC address of the access point on which the association failed and the number of association failures.
Severity	Major.
Category	Mesh
Probable Causes	The controller encountered excessive association failures.
Recommended Actions	None.

CISCO_LWAPP_MESH_PARENT_EXCLUDED_CHILD

MIB Name	ciscoLwappMeshParentExcludedChild
Alarm Condition	NA
NCS Message	Excluded by parent AP due to failed authentication.
Symptoms	When a child keeps failing authentication at the controller, the parent can mark that child for exclusion. The child cannot associate with the parent during this exclusion period. The trap contains the excluded child MAC address.
Severity	Informational
Category	Mesh
Probable Causes	A parent marked a child for exclusion.
Recommended Actions	None.

CISCO_LWAPP_MESH_CHILD_EXCLUDED_PARENT

MIB Name	ciscoLwappMeshChildExcludedParent
Alarm Condition	NA
NCS Message	Parent AP being excluded by child AP.
Symptoms	When a child fails authentication at the controller after a fixed number of attempts, the child can exclude that parent. The child remembers the excluded parent so that when it joins the network, it sends the trap which contains the excluded parent MAC address and the duration of the exclusion period.
Severity	Informational
Category	Mesh
Probable Causes	A child marked a parent for exclusion.
Recommended Actions	None.

CISCO_LWAPP_MESH_EXCESSIVE_PARENT_CHANGE

MIB Name	ciscoLwappMeshExcessiveParentChange
Alarm Condition	NA
NCS Message	Parent changed frequently.
Symptoms	When MAP parent-change-counter exceeds the threshold within a given duration, it sends a trap to the NCS. The trap contains the number of times the MAP changes and the duration of the time. The threshold is user configurable.
Severity	Major.
Category	Mesh
Probable Causes	The MESH access point changed its parent frequently.
Recommended Actions	None.

IDS_SHUN_CLIENT_TRAP

MIB Name	CISCO-LWAPP-IDS-MIB. CLIdsNewShunClient.
Alarm Condition	IDS Shun client.
NCS Message	The Cisco Intrusion Detection System "{0}" has detected a possible intrusion attack by the wireless client "{1}."
Symptoms	This trap is generated in response to a shun client clear alert originated from a Cisco IDS/IPs appliance ("{0}") installed in the data path between the wireless client ("{1}") and the intranet of the site.
Severity	Critical.
Category	Security
Probable Causes	The designated client is generating a packet-traffic pattern which shares properties with a well-known form of attack on the network of the customer.
Recommended Actions	Investigate the designated client and determine if it is an intruder, a virus, or a false alarm.

IDS_SHUN_CLIENT_CLEAR_TRAP

MIB Name	CISCO-LWAPP-IDS-MIB. cLIdsNewShunClientClear.
Alarm Condition	IDS Shun client clear.
NCS Message	The Cisco Intrusion Detection System "{0}" has cleared the wireless client "{1}" from possibly having generated an intrusion attack.
Symptoms	This trap is generated is response to one of two things: 1) a shun client clear alert originated from a Cisco IDS/IPS appliance ("{0}") installed in the data path between the wireless client ("{1"}) and the intranet of the site, or 2) a scheduled timeout of the original IDS_SHUN_CLIENT_TRAP for the wireless client.
Severity	Clear.
Category	Security

Probable Causes	The designated client is no longer generating a suspicious packet-traffic pattern.
Recommended Actions	None.

MFP_TIMEBASE_STATUS_TRAP

MIB Name	CISCO-LWAPP-MFP-MIB. ciscoLwappMfpTimebaseStatus.
Alarm Condition	MFP timebase out of sync.
NCS Message	Controller "{0}" is "{1}" with the Central time server.
Symptoms	This notification is sent by the agent to indicate when the synchronization of the time base of the controller with the Central time base last occurred.
Severity	Critical (not in sync trap) and clear (sync trap).
Category	Security
Probable Causes	The time base of the controller is not in sync with the Central time base.
Recommended Actions	None.

MFP_ANOMALY_DETECTED_TRAP

MIB Name	CISCO-LWAPP-MFP-MIB. ciscoLwappMfpAnomalyDetected.
Alarm Condition	MFP anomaly detected.
NCS Message	MFP configuration of the WLAN was violated by the radio interface "{0}" and detected by the radio interface "{1}" of the access point with MAC address "{2}." The violation is "{3}."
Symptoms	This notification is sent by the agent when the MFP configuration of the WLAN was violated by the radio interface cLApIfSmtDot11Bssid and detected by the radio interface cLApDot11IfSlotId of the access point cLApSysMacAddress. This violation is indicated by cLMfpEventType. When observing the management frame(s) given by cLMfpEventFrames for the last cLMfpEventPeriod time units, the controller reports the occurrence of a total of cLMfpEventTotal violation events of type cLMfpEventType. When the cLMfpEventTotal is 0, no further anomalies have recently been detected, and the NMS should clear any alarm raised about the MFP errors. **Note** This notification is generated by the controller only if MFP was configured as the protection mechanism through cLMfpProtectType.
Severity	Critical.
Category	Security
Probable Causes	The MFP configuration of the WLAN was violated. Various types of violations are invalidMic, invalidSeq, noMic, and unexpectedMic.
Recommended Actions	None.

GUEST_USER_REMOVED_TRAP

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserRemoved.
Alarm Condition	Guest user removed.
NCS Message	Guest user "{1}" deleted on controller "{0}."
Symptoms	This notification is generated when the lifetime of the guest user {1} expires and the guest user accounts are removed from the controller "{0}."

Severity	Critical.
Category	NCS
Probable Causes	GuestUserAccountLifetime expired.
Recommended Actions	None.

Traps Added or Updated in Release 4.0.96.0

The following traps were added in WCS Release 4.0.96.0:

- AP_IMPERSONATION_DETECTED, page 13-52
- RADIUS_SERVER_DEACTIVATED, page 13-52
- RADIUS_SERVER_ACTIVATED, page 13-52
- RADIUS_SERVER_WLAN_DEACTIVATED, page 13-53
- RADIUS_SERVER_WLAN_ACTIVATED, page 13-53
- RADIUS_SERVER_TIMEOUT, page 13-53
- DECRYPT_ERROR_FOR_WRONG_WPA_WPA2, page 13-53

AP_IMPERSONATION_DETECTED

MIB Name	bsnAPImpersonationDetected.
Alarm Condition	AP impersonation detected.
NCS Message	AP Impersonation with MAC "{0}" using source MAC "{1}" is detected by authenticated AP "{2}" on "{3}" radio and slot ID "{4}."
Symptoms	A radio of an authenticated access point had communication with another access point whose MAC address neither matches that of a rogue nor is an authenticated neighbor of the detecting access point.
Severity	Critical.
Category	Security
Probable Causes	A security breach related to access point impersonation might be occurring.
Recommended Actions	Track down the MAC address of the impersonating access point and contain it.

RADIUS_SERVER_DEACTIVATED

MIB Name	ciscoLwappAAARadiusServerGlobalDeactivated.
Alarm Condition	RADIUS Server deactivated.
NCS Message	RADIUS server "{0}" (port {1}) is deactivated.
Symptoms	The controller detects that the RADIUS server is deactivated in the global list.
Severity	Major.
Category	Controller
Probable Causes	RADIUS server is deactivated in the global list.
Recommended Actions	None.

RADIUS_SERVER_ACTIVATED

MIB Name	ciscoLwappAAARadiusServerGlobalDeactivated.
Alarm Condition	Radius server activated.
NCS Message	RADIUS server "{0}" (port {1}) is activated.
Symptoms	The controller detects that the RADIUS server is deactivated in the global list.
Severity	Clear.
Category	Controller
Probable Causes	RADIUS server is activated in the global list.
Recommended Actions	None.

RADIUS_SERVER_WLAN_DEACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanDeactivated.
Alarm Condition	RADIUS Server WLAN deactivated
NCS Message	RADIUS server "{0}" (port {1}) is deactivated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is deactivated on the WLAN.
Severity	Major.
Category	Controller
Probable Causes	RADIUS server is deactivated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_WLAN_ACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanActivated.
Alarm Condition	Radius server WLAN activated.
NCS Message	RADIUS server "{0}" (port {1}) is activated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is activated on the WLAN.
Severity	Clear.
Category	Controller
Probable Causes	RADIUS server is activated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_TIMEOUT

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusReqTimedOut.
Alarm Condition	RADIUS Server timeout.
NCS Message	RADIUS server "{0}" (port {1}) failed to respond to request from client "{2}" with MAC "{3}."
Symptoms	The controller detects that the RADIUS server failed to respond to a request from a client or user.
Severity	Informational.
Category	Controller
Probable Causes	RADIUS server fails to process the request from the client or user.
Recommended Actions	None.

DECRYPT_ERROR_FOR_WRONG_WPA_WPA2

MIB Name	CISCO-LWAPP-DOT11-CLIENT-MIB. CiscoLwappDot11ClientKeyDecryptError.
Alarm Condition	Client decrypt error occurred

NCS Message	Decrypt error occurred at AP with MAC "{0}" running TKIP with wrong WPA/WPA2 by client with MAC "{1}."
Symptoms	The controller detects that a user is trying to connect with an invalid security policy for WPA/WPA2 types.
Severity	Minor.
Category	Security
Probable Causes	The user failed to authenticate and join the controller.
Recommended Actions	None.

Traps Added or Updated in Release 4.1

The following traps were added for WCS Release 4.1:

- AP_IMPERSONATION_DETECTED, page 13-56
- INTERFERENCE_DETECTED, page 13-56
- INTERFERENCE_CLEAR, page 13-56
- ONE_ANCHOR_ON_WLAN_UP, page 13-57
- RADIUS_SERVER_DEACTIVATED, page 13-57
- RADIUS_SERVER_ACTIVATED, page 13-57
- RADIUS_SERVER_WLAN_DEACTIVATED, page 13-57
- RADIUS_SERVER_WLAN_ACTIVATED, page 13-59
- RADIUS_SERVER_TIMEOUT, page 13-59
- MOBILITY_ANCHOR_CTRL_PATH_DOWN, page 13-59
- MOBILITY_ANCHOR_CTRL_PATH_UP, page 13-59
- MOBILITY_ANCHOR_DATA_PATH_DOWN, page 13-61
- MOBILITY_ANCHOR_DATA_PATH_UP, page 13-61
- WLAN_ALL_ANCHORS_TRAP_DOWN, page 13-61
- MESH_AUTHORIZATIONFAILURE, page 13-61
- MESH_CHILDEXCLUDEDPARENT, page 13-62
- MESH_PARENTCHANGE, page 13-62
- MESH_PARENTEXCLUDECHILD, page 13-63
- MESH_CHILDMOVED, page 13-63
- MESH_EXCESSIVEASSOCIATIONFAILURE, page 13-63
- MESH_EXCESSIVEPARENTCHANGE, page 13-64
- MESH_POORSNR, page 13-64
- MESH_POORSNRCLEAR, page 13-65
- MESH_CONSOLELOGIN, page 13-65
- LRADIF_REGULATORY_DOMAIN, page 13-65
- LRAD_CRASH, page 13-66

- LRAD_UNSUPPORTED, page 13-66

AP_IMPERSONATION_DETECTED

MIB Name	bsnAPImpersonationDetected.
Alarm Condition	AP impersonation detected.
NCS Message	AP impersonation of MAC "{0}" using source MAC "{1}" is detected by an authenticated AP "{2}" on "{3}" radio and slot ID "{4}."
Symptoms	A radio of an authenticated access point received signals from another access point whose MAC address neither matches that of a rogue nor is an authenticated neighbor of the detecting access point.
Severity	Critical.
Category	Access Point..
Probable Causes	A security breach related to access point impersonation has occurred.
Recommended Actions	Track down the MAC address of the impersonating access point and contain it.

INTERFERENCE_DETECTED

MIB Name	cognioInterferenceAlarm.
Alarm Condition	None.
NCS Message	Interference detected by type {0} with power {1}.
Symptoms	A Cognio spectrum agent detected interference over its configured thresholds.
Severity	Minor.
Category	SE Detected Interferers
Probable Causes	Excessive wireless interference or noise.
Recommended Actions	None.

INTERFERENCE_CLEAR

MIB Name	COGNIO-TRAPS-MIB. cognioInterferenceClear
Alarm Condition	None.
NCS Message	Interference cleared.
Symptoms	The Cognio spectrum expert agent no longer detects an interference source over its configured threshold.
Severity	Clear.
Category	SE Detected Interferers
Probable Causes	Previous excessive wireless interference or noise is gone.
Recommended Actions	None.

ONE_ANCHOR_ON_WLAN_UP

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityOneAnchorOnWlanUp.
Alarm Condition	
NCS Message	Controller "{0}." An anchor of WLAN "{1}" is up.
Symptoms	Successive EoIP and UDP ping to at least one anchor on the WLAN is up.
Severity	Clear.
Category	Controller
Probable Causes	At least one anchor is reachable from an EoIP/UDP ping.
Recommended Actions	None.

RADIUS_SERVER_DEACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerGlobalDeactivated.
Alarm Condition	RADIUS Server deactivated.
NCS Message	RADIUS server "{0}" (port {1}) is deactivated.
Symptoms	The controller detects that the RADIUS server is deactivated in the global list.
Severity	Major.
Category	Controller
Probable Causes	RADIUS server is deactivated in the global list.
Recommended Actions	None.

RADIUS_SERVER_ACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerGlobalActivated.
Alarm Condition	Radius server activated.
NCS Message	RADIUS server "{0}" (port {1}) is activated.
Symptoms	The controller detects that the RADIUS server is activated in the global list.
Severity	Clear.
Category	Controller
Probable Causes	RADIUS server is activated in the global list.
Recommended Actions	None.

RADIUS_SERVER_WLAN_DEACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanDeactivated.
Alarm Condition	Radius server WLAN deactivated.

NCS Message	RADIUS server "{0}" (port {1}) is deactivated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is deactivated on the WLAN.
Severity	Major.
Category	Controller
Probable Causes	RADIUS server is deactivated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_WLAN_ACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerGlobalWlanActivated.
Alarm Condition	Radius server WLAN activated.
NCS Message	RADIUS server "{0}" (port {1}) is activated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is activated on the WLAN.
Severity	Clear.
Category	Controller
Probable Causes	RADIUS server is activated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_TIMEOUT

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusReqTimedOut.
Alarm Condition	RADIUS Server timeout.
NCS Message	RADIUS server "{0}" (port {1}) failed to respond to request from client "{2}" with MAC "{3}."
Symptoms	The controller detects that the RADIUS server failed to respond to a request from the client or user.
Severity	Informational.
Category	Controller
Probable Causes	The RADIUS server fails to process the request from a client or user.
Recommended Actions	None.

MOBILITY_ANCHOR_CTRL_PATH_DOWN

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorControlPathDown.
Alarm Condition	Mobility anchor control path down.
NCS Message	Controller "{0}." Control path on anchor "{1}" is down.
Symptoms	When successive ICMP ping attempts to the anchor fails, the anchor is conclusively down.
Severity	Major.
Category	Controller
Probable Causes	Anchor not reachable by ICMP ping.
Recommended Actions	None.

MOBILITY_ANCHOR_CTRL_PATH_UP

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorControlUp.
Alarm Condition	Mobility anchor control path up.

NCS Message	Controller "{0}." Control path on anchor "{1}" is up.
Symptoms	The ICMP ping to the anchor is restored, and the anchor is conclusively up.
Severity	Clear.
Category	Controller
Probable Causes	The anchor is reachable by an ICMP ping.
Recommended Actions	None.

MOBILITY_ANCHOR_DATA_PATH_DOWN

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorDataPathDown.
Alarm Condition	Mobility anchor data path down.
NCS Message	Controller "{0}." Data path on anchor "{1}" is down.
Symptoms	Successive EoIP ping attempts to the anchor fails, and the anchor is conclusively down.
Severity	Major.
Category	Controller
Probable Causes	The anchor is not reachable by an EoIP ping.
Recommended Actions	None.

MOBILITY_ANCHOR_DATA_PATH_UP

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorDataPathUp.
Alarm Condition	Mobility anchor data path up.
NCS Message	Controller "{0}." Data path on anchor "{1}" is up.
Symptoms	The EoIP ping to the anchor is restored, and the anchor is conclusively up.
Severity	Clear.
Category	Controller
Probable Causes	Anchor is reachable by the EoIP ping.
Recommended Actions	None.

WLAN_ALL_ANCHORS_TRAP_DOWN

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAllAnchorsOnWlanDown.
Alarm Condition	WLAN all anchors down.
NCS Message	Controller "{0}." All anchors of WLAN "{1}" are down.
Symptoms	Successive EoIP ping attempts to all the anchors on WLAN is occurring.
Severity	Critical.
Category	Controller
Probable Causes	Anchors are not reachable by the EoIP ping.
Recommended Actions	None.

MESH_AUTHORIZATIONFAILURE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshAuthorizationFailure.
Alarm Condition	Mesh authorization failure.
NCS Message	MESH "{0}" fails to authenticate with controller because "{1}".
Symptoms	A mesh access point failed to join the mesh network because its MAC address is not listed in the MAC filter list. The alarm includes the MAC address of the mesh access point that failed to join.
Severity	Minor.
Category	Mesh
Probable Causes	The mesh node MAC address is not in the MAC filter list, or a security failure from the authorization server occurred.
Recommended Actions	None.

MESH_CHILDEXCLUDEDPARENT

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshChildExcludedParent.
Alarm Condition	Mesh child exclude parent.
NCS Message	Parent AP being excluded by child AP due to failed authentication, AP current parent MAC address "{0}," previous parent MAC address "{1}."
Symptoms	This notification is sent by the agent when the child access point marks a parent access point for exclusion. When the child fails to authenticate at the controller after a fixed number of times, the child marks the parent for exclusion. The child remembers the excluded MAC address and informs the controller when it joins the network. The child access point marks the MAC address and excludes it for the time determined by MAP node so that it does not try to join this excluded node. The child MAC address is sent as part of the index.
Severity	Informational
Category	Mesh
Probable Causes	The child access point failed to authenticate to the controller after a fixed number of times.
Recommended Actions	None.

MESH_PARENTCHANGE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshParentChange.
Alarm Condition	Mesh parent change.
NCS Message	MESH "{0}" changed its parent. AP current parent MAC address "{1}," previous parent MAC address "{2}."
Symptoms	This notification is sent by the agent when a child moves to another parent. The alarm includes the MAC addresses of the former and current parents.
Severity	Informational

Category	Mesh
Probable Causes	The child access point has changed its parent.
Recommended Actions	None.

MESH_PARENTEXCLUDECHILD

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshParentExcludedChild
Alarm Condition	NA
NCS Message	MESH "{0}" being excluded by parent AP due to failed authentication. AP neighbor type "{1}".
Symptoms	This notification is sent by the agent when the parent AP marks a child to be excluded. When child keeps failing authentication at controller, parent can mark child to be excluded for configured value for 'clMeshExclusionTimeout', so that child does not associate again with the parent.
Severity	Informational
Category	Mesh
Probable Causes	Child keeps failing authentication at controller.
Recommended Actions	None.

MESH_CHILDMOVED

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshChildMoved.
Alarm Condition	Mesh child removed.
NCS Message	Parent AP "{0}" lost connection to AP "{1}". AP neighbor type is "{2}".
Symptoms	This notification is sent by the agent when the parent access point loses connection with its child.
Severity	Informational.
Category	Mesh
Probable Causes	The parent access point lost connection with its child.
Recommended Actions	None.

MESH_EXCESSIVEASSOCIATIONFAILURE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshExcessiveAssociationFailure
Alarm Condition	Mesh excessive association failure.
NCS Message	MESH "{0}" has excessive association failures.

Symptoms	This notification is sent by the agent when the cumulative association failures of child APs exceeds value configured in 'clMeshExcessiveAssociationFailure'
Severity	Major
Category	Mesh
Probable Causes	This can happen when the cumulative association failure of child APs exceeds value configured in 'clMeshExcessiveAssociationFailure'.
Recommended Actions	None.

MESH_EXCESSIVEPARENTCHANGE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshExcessiveParentChange.
Alarm Condition	Mesh excessive parent change.
NCS Message	MESH "{0}" changes parent frequently.
Symptoms	This notification is sent by the agent if the number of parent changes for a given mesh access point exceeds the threshold. Each access point keeps count of the number of parent changes within a fixed time. If the count exceeds the threshold defined by c1MeshExcessiveParentChangeThreshold, then the child access point informs the controller.
Severity	Major.
Category	Mesh
Probable Causes	The child access point has frequently changed its parent.
Recommended Actions	None.

MESH_POORSNR

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshPoorSNR.
Alarm Condition	Mesh Poor SNR.
NCS Message	MESH "{0}" has SNR on backhaul link as "{1}" which is lower then predefined threshold.
Symptoms	This notification is sent by the agent when the child access point detects a signal-to-noise ratio below 12dB the backhaul link. The alarm includes the SNR value and the MAC addresses of the parent and child.
Severity	Major.
Category	Mesh
Probable Causes	SNR is lower then the threshold defined by c1MeshSNRThreshold.
Recommended Actions	None.

MESH_POORSNRCLEAR

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshPoorSNRClear.
Alarm Condition	Mesh Poor SNR clear.
NCS Message	MESH "{0}" has SNR on backhaul link as "{1}" which is normal now.
Symptoms	This notification is sent by the agent to clear ciscoLwappMeshPoorSNR when the child access point detects SNR on the backhaul link that is higher than the threshold defined by c1MeshSNRThreshold.
Severity	Clear.
Category	Mesh
Probable Causes	SNR on the backhaul link is higher than the threshold defined by c1MeshSNRThreshold.
Recommended Actions	None.

MESH_CONSOLELOGIN

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshConsoleLogin.
Alarm Condition	Mesh console login.
NCS Message	MESH "{0}" has console logged in with status "{1}".
Symptoms	This notification is sent by the agent when login on the MAP console is successful or when a failure occurred after three attempts.
Severity	Critical.
Category	Mesh
Probable Causes	Login on the MAP console was successful, or a failure occurred after three attempts.
Recommended Actions	None.

LRADIF_REGULATORY_DOMAIN

MIB Name	ciscoLwappApIfRegulatoryDomainMismatchNotif
Alarm Condition	Radio interface regulatory domain mismatch.
NCS Message	Access Point "{0}" is unable to associate. The Regulatory Domain "{1}" configured on interface "{2}" does not match the controller "{3}" regulatory domain "{4}."
Symptoms	The system generates this trap when the regulatory domain configured on the access point radios does not match the country code configured on the controller.
Severity	Critical.
Category	Access Point.

Probable Causes	If the country code configuration of the controller is changed, and some access points support a different country code, then these access points fail to associate. An access point on the network of the controller sends join requests to the controller, but the regulatory domain is outside the domain in which the controller is operating.
Recommended Actions	Either remove the access points that are not meant for inclusion in the domain of the controller or correct the country code setting of the controller.

LRAD_CRASH

MIB Name	ciscoLwappApCrash
Alarm Condition	Access point crash.
NCS Message	Access Point "{0}" crashed and has a core dump on controller "{1}."
Symptoms	An access point has crashed.
Severity	Informational.
Category	Access Point.
Probable Causes	Access point failure.
Recommended Actions	Capture the core dump file using the command-line interface of the controller and send it to TAC support.

LRAD_UNSUPPORTED

MIB Name	ciscoLwappApUnsupported
Alarm Condition	Access point not supported.
NCS Message	Access Point "{0}" tried to join controller "{1}" and failed. Associate failure reason "{2}."
Symptoms	An access point tried to associate to a controller to which it is not supported.
Severity	Informational.
Category	Access Point.
Probable Causes	The access point is not supported by the controller.
Recommended Actions	None.

Traps Added or Updated in Release 4.2

The following traps were added to WCS Release 4.2:

- GUEST_USER_ADDED, page 13-67
- GUEST_USER_AUTHENTICATED, page 13-67
- IOSAP_LINK_UP, page 13-67
- LRAD_POE_STATUS, page 13-68

- ROGUE_AP_NOT_ON_NETWORK, page 13-68
- IOSAP_UP, page 13-68

GUEST_USER_ADDED

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserAdded
Alarm Condition	Guest user added.
NCS Message	Guest user "{0}" created on the controller “{1}.”
Symptoms	This notification is sent by the agent when the GuestUser account is created successfully.
Severity	Informational.
Category	Controller
Probable Causes	The guest user account was created on the agent by either command-line interface, Web UI, or NCS.
Recommended Actions	None.

GUEST_USER_AUTHENTICATED

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserLogged
Alarm Condition	Guest user authenticated.
NCS Message	Guest user "{1}" logged into controller "{0}."
Symptoms	This notification is sent by the agent when the GuestUser logged into the network through webauth successfully.
Severity	Informational.
Category	Controller
Probable Causes	The guest user was successful with webauth authentication.
Recommended Actions	None.

IOSAP_LINK_UP

MIB Name	linkUp
Alarm Condition	Autonomous AP Link Up.
NCS Message	Autonomous AP “{0},” Interface “{1}” is {2} up.
Symptoms	The physical link is up on an autonomous access point radio port.
Severity	Clear.
Category	Access Point.
Probable Causes	A physical link has been restored to the autonomous access point.
Recommended Actions	None.

LRAD_POE_STATUS

MIB Name	ciscoLwappApPower
Alarm Condition	POE Status.
NCS Message	Access point “{0}” draws low power from Ethernet. Failure reason: “{1}”
Symptoms	This notification is generated when the access point draws low power from the Ethernet connection.
Severity	Critical.
Category	Access Point.
Probable Causes	The access point receives low power from the Ethernet connection.
Recommended Actions	Check the power status of the access point and the device connected to the access point.

ROGUE_AP_NOT_ON_NETWORK

MIB Name	bsnRogueAPDetectedOnWiredNetwork (bsnRogueAPOnWiredNetwork is set to false).
Alarm Condition	ROGUE_AP_NOT_ON_NETWORK
NCS Message	Rogue AP or ad hoc rogue "{0}" is not able to connect to the wired network.
Symptoms	A rogue access point is no longer on the wired network.
Severity	Informational.
Category	Rogue AP
Probable Causes	The rogue access point is no longer reachable on the wired network.
Recommended Actions	None.

IOSAP_UP

MIB Name	None.
Alarm Condition	Autonomous AP Up.
NCS Message	The autonomous AP “{0}” is reachable.
Symptoms	The autonomous AP is SNMP reachable.
Severity	Clear.
Category	Access Point.
Probable Causes	The autonomous access point starts to respond to SNMP queries.
Recommended Actions	None.

Traps Added or Updated in Release 5.0

The following traps were added for WCS Release 5.0:

GUEST_USER_LOGOFF

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserLoggedOut
Alarm Condition	Guest user logged off.
NCS Message	Guest user "{1}" logged out from the controller "{0}."
Symptoms	This notification is sent by the agent when a GuestUser who was previously logged into the network logs out.
Severity	Informational.
Category	Controller
Probable Causes	The GuestUser logs off from the network.
Recommended Actions	None.

STATION_ASSOCIATE_DIAG_WLAN

MIB Name	CISCO-LWAPP-DOT11-CCX-CLIENT-MIB.cldccDiagClientAssociatedToDiagWlan
Alarm Condition	Client Associated to Diagnostic Channel.
NCS Message	Client "{0}" is associated to diagnostic WLAN with reason "{1}."
Symptoms	This notification is sent by the agent when a v5 client associates to a diagnostic channel.
Severity	Informational.
Probable Causes	When a CCXv5 client gets associated to the diagnostic channel WLAN on WLC, this trap is raised.
Category	Clients
Recommended Actions	If you want to automatically perform client troubleshooting, you must enable Client Troubleshooting in Administration > Settings > client. After it is enabled, the series of V5 tests are carried out on the client upon trap arrival, and the client is updated with the test status through pop-up messages. The report is placed in the logs directory. The log filename is shown in the Client Details page in the Automated Troubleshooting Report section. You can export all automated troubleshooting logs.

Traps Added or Updated in Release 5.2

The following traps were added for WCS Release 5.2:

LRAD_REBOOTREASON

MIB Name	ciscoLwappApAssociated
Alarm Condition	AP reboot reason.
NCS Message	Access Point ''{0}'' associated to controller ''{2}'' on port number ''{1}''. Reason for association ''{3}''.
Symptoms	
Severity	Informational
Category	Access Point.
Probable Causes	None.
Recommended Actions	None.

WIPS_TRAPS

MIB Name	ciscoLwappIpsMIBNotif
Alarm Condition	wIPS Traps.
NCS Message	Dynamically generated per alarm.
Symptoms	See the wIPS alarm encyclopedia under NCS > Configuration > wIPS Profiles.
Severity	Critical
Category	Security
Probable Causes	Possible security attacks.
Recommended Actions	None.

Alarm Names

- DoS: Association flood
- DoS: Association table overflow
- DoS: Authentication flood
- DoS: EAPOL-Start attack
- DoS: PS-Poll flood
- DoS: Unauthenticated association
- DoS: CTS flood
- DoS: Queensland University of Technology Exploit
- DoS: RF jamming
- DoS: RTS flood
- DoS: Virtual Carrier attack

- DoS: Authentication-failure attack
- DoS: De-Auth broadcast flood
- DoS: De-Auth flood
- DoS: Dis-Assoc broadcast flood
- DoS: Dis-Assoc flood
- DoS: EAPOL-Logoff attack
- DoS: FATA-Jack tool
- DoS: Premature EAP-Failure
- DoS: Premature EAP-Success
- ASLEAP tool detected
- Airsnarf attack
- ChopChop attack
- Day-Zero attack by WLAN security anomaly
- Day-Zero attack by device security anomaly
- Device probing for APs
- Dictionary attack on EAP methods
- Fake APs detected
- Fake DHCP server detected
- Fast WEP crack tool detected
- Fragmentation attack
- Honeypot AP detected
- Hotspotter tool detected
- Hotspotter tool detected
- Malformed 802.11 packets detected
- Man in the middle attack
- NetStumbler detected
- Netstumbler victim detected
- PSPF violation detected
- Soft AP or host AP detected
- Spoofed MAC address detected
- Suspicious after-hours traffic detected
- Unauthorized association by vendor list
- Unauthorized association detected
- Wellenreiter detected

Traps Added or Updated in Release 6.0

The following traps were added for WCS Release 6.0:

MSE_EVAL_LICENSE

MIB Name	None
Alarm Condition	MSE Evaluation license expired.
NCS Message	Evaluation license for {0} is expired.
Symptoms	The tracking for clients or tags stops, or service does not come up.
Severity	Critical.
Category	MSE
Probable Causes	The evaluation period for the service has expired.
Recommended Actions	Add a permanent license for the service using License Center or the appropriate third-party vendor application.

MSE_LICENSING_ELEMENT_LIMIT

MIB Name	None
Alarm Condition	MSE Licensing element limit reached.
NCS Message	{0} limit for {1} is reached or exceeded.
Symptoms	Elements are not tracked beyond a certain limit.
Severity	Critical.
Category	MSE
Probable Causes	Limit for the specified service has been reached.
Recommended Actions	Add a license with higher licensed capacity for the particular service.

STATION_AUTHENTICATED

MIB Name	ciscoLwappDot11ClientMovedToRunState
Alarm Condition	Client Authentication failure.
NCS Message	Client “{0}” is authenticated with interface “{2}” of AP “{1}.”
Symptoms	A client has completed a security policy and has moved to Run state. It can start to send or receive data.
Severity	Informational.
Category	Wired Clients.
Probable Causes	A client has completed security policy and moved to Run state.
Recommended Actions	None.

WLC_LICENSE_NOT_ENFORCED

MIB Name	clmgmtLicenseNotEnforced
Alarm Condition	Attempt to use an unlicensed Controller feature.
NCS Message	Controller {0} has AP with unlicensed feature {1} version {2} attempting to join.

Symptoms	An access point with a licensed feature is trying to join a controller without the proper license.
Severity	Critical.
Category	Controller
Probable Causes	An access point with a WPLUS feature like indoor mesh or OfficeExtend AP is trying to join a controller without a WPLUS license.
Recommended Actions	You must add a WPLUS license to the controller or fix the primary, secondary, or tertiary controller configuration to have controllers with WPLUS licenses.

WLC_LICENSE_COUNT_EXCEEDED

MIB Name	clmgmtLicenseUsageCountExceeded
Alarm Condition	AP attempted to join Controller with licensed AP count exceeded.
NCS Message	Controller {0} with license {1} version {2} and counted feature {4} with limit {3} has been exceeded {5}.
Symptoms	The access point cannot join a controller.
Severity	Critical.
Category	Controller
Probable Causes	The controller has reached the maximum licensed access point capacity.
Recommended Actions	Add a license capacity to the controller or move the access point to a controller with more capacity.

VOIP_CALL_FAILURE

MIB Name	ciscoLwappVoipCallfailureNotif
Alarm Condition	VoIP Call failed.
NCS Message	VoIP Call failure of {4} (Error Code {3}) occurred on Client {0} with phone number {5} calling {6} which was associated with AP {1} on interface {2}.
Symptoms	VoIP snooping is enabled on a WLAN.
Severity	Informational.
Category	Clients
Probable Causes	A SIP error is detected by an access point.
Recommended Actions	The actions depend on the type of error that is being reported. Errors can range from “dialed number does not exist,” “busy,” “service unavailable,” to “service timeout.”

Traps Added or Updated in Release 7.0

The following traps were added for WCS Release 7.0:

- SI_AQ_TRAPS, page 13-76
- SI_SECURITY_TRAPS, page 13-76

- SI_SENSOR_CRASH_TRAPS, page 13-76

SI_AQ_TRAPS

MIB Name	ciscoLwappSiAqLow
Alarm Condition	Air Quality Traps
NCS Message	Air Quality Index on Channel {0} is {1} (Threshold: {2}).
Symptoms	Air Quality fall below the set Threshold.
Severity	Minor.
Category	Performance.
Probable Causes	Threshold is set via the configuration->controller->CleanAir. When the Air Quality Index computed by the AP falls below the set threshold this is triggered.
Recommended Actions	Detect Source of Interference and remove it from the environment or enable RRM so that AP can move to another clean channel.

SI_SECURITY_TRAPS

MIB Name	ciscoLwappSiIdrDevice
Alarm Condition	Interferer Security Traps.
NCS Message	Set: Security-Risk Interferer {0} is detected. Clear: Security-risk Interferer "{0}" is no longer detected.
Symptoms	Raised when Interferer marked as a security threat is detected by the network.
Severity	Critical.
Category	Security
Probable Causes	Interferer marked as a security threat is detected by the network. Interferers have to configured to as Security threat and it can be done via the configuration->controller->CleanAir section.
Recommended Actions	Detect Source of Interference and remove it from the environment.

SI_SENSOR_CRASH_TRAPS

MIB Name	ciscoLwappSiSensorCrash
Alarm Condition	Sensor Crash Traps
NCS Message	CleanAir Sensor Status: {0} Error Code: {1}.
Symptoms	CleanAir Sensor Software stopped working.
Severity	Critical.
Category	Access Point.
Probable Causes	General Sensor crashes.
Recommended Actions	Reboot the AP.

Traps Added or Updated in Release 7.0.1

The following traps were added to WCS Release 7.0.1:

FAN_MONITOR

MIB Name	None.
Alarm Condition	Fan Monitor on MSE
Category	Mobility Services
Symptoms	A system cooling fan gone bad.
Severity	Critical
NCS Message	Cooling fan failure [applies to MSE-3355 only]. One of the CPU cooling fans on $HOST [$IP] has failed.
Probable Causes	Failure of a fan.
Recommended Actions	Customer should contact Cisco TAC to arrange for replacing the system. This failure cannot be fixed in the field (fan is not replaceable).

FUTURE_RESTART_DAY_MSG

MIB Name	None.
Alarm Condition	MSE Restart
Category	Mobility Service
Symptom	None.
Severity	Major
NCS Message	The MSE {0} will be restarted on {date} at {time} am/pm.
Probable Causes	Planned restart for password refresh to prevent Oracle db locking.
Recommended Actions	None.

MIB Name	None.
Alarm Condition	MSE Restart
Category	Mobility Service
Symptom	The NCS reported lost connectivity or MSE became unreachable momentarily.
Severity	Major
NCS Message	The MSE {0} was restarted on {date}.
Probable Causes	Planned restart for password refresh to prevent Oracle db locking.
Recommended Actions	None.

LOCATION_CALCULATOR

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Failed to complete the heatmap calculation process.
Symptoms	Missing device locations. Inaccurate device location.
Severity	Major
Category	Mobility Service
Probable Causes	Matlab process crash.
Recommended Actions	None. System tries to correct itself every 2 hours. If needed resync the floors to the MSE.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Recovered from Matlab crash and completed the heatmap calculation process.
Symptoms	Devices start showing up or location is more accurate.
Severity	Clear
Category	Mobility Service
Probable Causes	Matlab process crash.
Recommended Actions	System recovered from a previous crash.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.

NCS Message	HEATMAP_CALCULATION_ERROR The data set in the calibration is not initialized properly for Calibration Model (Name, id): {0}, {1}.
Symptoms	Poor location accuracy.
Severity	Major
Category	Mobility Service
Probable Causes	Calibration data pushed from the NCS to MSE not good.
Recommended Actions	Reapply calibration model to the floor and resync to the MSE. Worst case, redo calibration.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Recovered from calibration error for model (Name, Id): {0}, {1}.
Symptoms	Improved location accuracy.
Severity	Clear
Category	Mobility Service
Probable Causes	System recovered from a previous calibration error due to resync.
Recommended Actions	None.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Failed to calculate Heatmap for AP Interface {0}. Falling back to using default heatmap.
Symptoms	No location for device or poor location accuracy.
Severity	Major
Category	Mobility Service
Probable Causes	Bad AP Data like antenna type, antenna pattern, and so on.
Recommended Actions	Correct AP antenna type/pattern of the AP Interface and resync the floor with the error AP to MSE. Enable Default Heatmaps Calculation from Context Aware Service > Location Parameters page and resync the floor with the error AP to MSE.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Successful heatmap computation for AP Key {0}.

Symptoms	Devices start showing up or location is more accurate.
Severity	Clear
Category	Mobility Service
Probable Causes	System recovered from a previous heatmap calculation error.
Recommended Actions	None.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR No Rails and Regions input specified for AP interface for floor (name, id): {0}, {1}.
Symptoms	Device show outside or inside unexpected areas on the maps.
Severity	Informational
Category	Mobility Service
Probable Causes	Default inclusion region was deleted from floor map.
Recommended Actions	Recreate the inclusion area on the floor map.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Rails and Regions added back to floor (name, id): {0}, {1}.
Symptoms	Devices locations are always constrained within the floor map inclusion region boundary.
Severity	Clear
Category	Mobility Service
Probable Causes	Inclusion region was added back to the floor map.
Recommended Actions	None.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Heatmap generated for AP Interface: {0} is not a location heatmap.
Symptoms	Devices not showing up.
Severity	Minor
Category	Mobility Service

Probable Causes	Mostly system error.
Recommended Actions	None. System tries to auto correct itself after 2 hours.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Successful heatmap computation of AP Key: {0}.
Symptoms	Devices start showing up.
Severity	Clear
Category	Mobility Service
Probable Causes	System recovered from a previous heatmap calculation error.
Recommended Actions	None.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Skipping default heatmap creation for AP Interface {0}.
Symptoms	No location for device or poor location accuracy.
Severity	Major
Category	Mobility Service
Probable Causes	Use of unknown Antenna pattern or non cisco antennas and use of default heatmaps is disabled.
Recommended Actions	Enable default heatmap calculation from Context Aware Service-> Location parameters page.

MIB Name	None.
Alarm Condition	Location Calculator on MSE.
NCS Message	HEATMAP_CALCULATION_ERROR Floor (name): {0} was deleted.
Symptoms	No location for device.
Severity	Clear
Category	Mobility Service
Probable Causes	Floor with heatmap calculation error was deleted.
Recommended Actions	None.

RAID_MONITOR

MIB Name	None.
Alarm Condition	RAID Monitor on MSE.
Category	Mobility Services
Symptoms	One of the disks in a RAID array has failed, as reported by the RAID controller.
Severity	Critical
NCS Message	A Hard Disk in a RAID set has failed. This applies to all three [3310, 3350, 3355] platforms. One of the hard drives on $HOST [$IP] has failed and must be replaced. Contact Cisco Customer Support immediately for assistance.
Probable Causes	Failure of a disk drive.
Recommended Actions	Replace the failed drive (if 3350, 3355) with a new hard drive, or setup an RMA with Cisco (for 3310). The new drive is automatically rebuilt (3355, 3350) by the RAID controller. For 3310, field replacement of the drive is NOT supported.

POWER_MONITOR

MIB Name	None.
Alarm Condition	Power Monitor on MSE.
NCS Message	No power supply redundancy [applies to MSE-3355 only]. One of the power supplies on $HOST [$IP] is not connected to a power source.
Symptoms	System has two power supplies but only one of them is connected to a power source.
Severity	Critical
Category	Mobility Services
Probable Causes	None.
Recommended Actions	Customer should connect the power supply to a good power source.

MIB Name	None.
Alarm Condition	Power Monitor on MSE.
NCS Message	Power supply missing or failed [applies to MSE-3355 only] Message Detail: One of the power supplies on $HOST [$IP] has failed or is missing." >.
Symptoms	System has two power supplies but one of them has failed or one of them has been physically removed.

Severity	Critical
Category	Mobility Service
Probable Causes	Bad or missing power supply.
Recommended Actions	Customer should check the power supplies and if it has failed, then replace it with a good one. Power supplies are spare items than can be ordered by customers. If the power supply is missing, then do the obvious.

SI_AQ_BUFFER_UNAVAILABLE_TRAPS

MIB Name	ciscoLwappSiAqBufferUnavailable
Alarm Condition	AQ Buffer unavailable on controller.
NCS Message	The NCS MESSAGE (RAISE): AQ data for AP "{0}" interface "{1}" is not available as AQ buffer allocation limit ("{2}") on controller has reached or AQ data allocation failed. The NCS MESSAGE (CLEAR): Allocation for AQ buffer successful, AQ data is now available for AP "{0}" interface "{1}".
Symptoms	This notification is generated if Air Quality buffer is unavailable.
Severity	Warning.
Category	Controller
Probable Causes	Controller Resource limitation.
Recommended Actions	None.

NCS_NOTIFICATION_ALARM

MIB Name	ciscoWirelessMOStatusNotification
Alarm Condition	The NCS notification alarm.
NCS Message	The NCS Message varies depending on the different HM sub category of the trap.
Symptoms	Health Monitor uses this trap to send notification to the NCS to indicate the Health Monitor alarm during various operation phases. • HM_DATABASE • HM_DATABASE_CRITICAL • HM_FAILBACK • HM_FAILOVER • HM_REACHABILITY • HM_REGISTRATION
Severity	• HM_DATABASE—Major • HM_DATABASE_CRITICAL—Critical • HM_FAILBACK—Major • HM_FAILOVER-Major • HM_REACHABILITY—Major • HM_REGISTRATION—Major
Category	High Availability

Probable Causes	• HM_DATABASE_CRITICAL—The database is down and cannot be started by HM. • HM_DATABASE—At the Database level, the connection between primary and secondary is lost. • HM_FAILBACK—Failback attempt failed. • HM_ FAILOVER -Failover attempt failed. • HM_REACHABILITY—Primary and Secondary cannot reach each other. • HM_REGISTRATION—Failed HA registration due to invalid authentication parameters.
Recommended Actions	• HM_DATABASE_CRITICAL—Check the database and the NCS log files for more information. • HM_DATABASE—Check the database and the NCS log files for more information. • HM_FAILBACK—Check the NCS log file for more information. • HM_ FAILOVER—Check the NCS log file for more information. • HM_REACHABILITY—Ensure that network connectivity is functioning. • HM_REGISTRATION—Ensure that the authentication key, version number, OS platform are all correct.

NMSP

MIB Name	None.
Alarm Condition	NMSP Connection Status.
NCS Message	NMSP Connection Status: INACTIVE, Controller IP: {0}.
Symptoms	Devices associated with this controller are not located by MSE.
Severity	Critical.
Category	Mobility Services
Probable Causes	Controller not reachable from MSE, Controller in read-only mode on the NCS, Controller and MSE are not NTP time synched.
Recommended Actions	Check NMSP Connection Status troubleshooting wizard for suggestions to fix the problem. Click the Tools link next to an inactive connection to open the wizard.

MIB Name	None.
Alarm Condition	NMSP Connection Status.
NCS Message	NMSP Connection Status: INACTIVE, Controller IP: {0}.
Symptoms	Device from Controller associated with the MSE show up.

Severity	Clear.
Category	Mobility Services
Probable Causes	NMSP Connection was reestablished between the MSE and the Controller or Switch.
Recommended Actions	None.

MSE_DOWN

MIB Name	None.
Alarm Condition	MSE down
NCS Message	MSE <Name> with IP Address <IPAddress> on port <port number> is unreachable.
Symptoms	Communication with MSE is not happening.
Severity	Major.
Category	Mobility Services
Probable Causes	This alarm is generated when the MSE or the LBS is unreachable from the NCS.
Recommended Actions	Ensure that the MSE Service is network reachable from the NCS and services on MSE are running correctly.

Traps Added in the NCS Release 1.0

The following traps were added in the NCS 1.0:

- AP_FUNCTIONALITY_LICENSE_EXPIRED, page 13-87
- AP_IP_FALLBACK, page 13-88
- COUNTRY_CODE_CHANGED, page 13-88
- CPU_RX_MULTICAST_QUEUE_FULL, page 13-88
- FAN_FAILURE, page 13-89
- GUEST_USER_REMOVED, page 13-89
- HEART_BEAT_LOSS, page 13-89
- IPSEC_ESP_AUTH_FAILURE, page 13-90
- IPSEC_ESP_INVALID_SPI, page 13-90
- IPSEC_ESP_REPLAY_FAILURE, page 13-90
- IPSEC_SUITE_NEG_FAILURE, page 13-91
- INVALID_RADIO, page 13-91
- LINK_FAILURE, page 13-91
- MESH_BATTERY, page 13-92
- MESH_DEFAULTBRIDGEGROUPNAME, page 13-92

AP_FUNCTIONALITY_LICENSE_EXPIRED

MIB Name	bsnAPFunctionalityDisabled
Alarm Condition	AP functionality license expired.
NCS Message	AP functionality has been disabled for key ‘’{0}’’ reason being ‘’{1}’’ for feature-set ‘’{2}’’.
Symptoms	None.
Severity	Critical
Category	Controller
Probable Causes	None.
Recommended Actions	None.

AP_IP_FALLBACK

MIB Name	bsnAPIPAddressFallback
Alarm Condition	AP IP fallback.
NCS Message	AP "{0}" with static-ip configured as "{2}" has fallen back to the working DHCP address "{1}".
Symptoms	None.
Severity	Minor
Category	Access Point.
Probable Causes	None.
Recommended Actions	None.

COUNTRY_CODE_CHANGED

MIB Name	countryChangeTrap
Alarm Condition	Country code changes.
NCS Message	Controller "{0}". Country code changed to "{1}".
Symptoms	None.
Severity	Information
Category	Controller
Probable Causes	None.
Recommended Actions	None.

CPU_RX_MULTICAST_QUEUE_FULL

MIB Name	bsnRxMulticastQueueFull
Alarm Condition	CPU RX Multicast queue full.
NCS Message	CPU Receive Multicast Queue is full on Controller ‘’{0}’’.
Symptoms	None.
Severity	Critical
Category	Controller
Probable Causes	None.
Recommended Actions	None.

FAN_FAILURE

MIB Name	fanFailureTrap
Alarm Condition	Fan failure.
NCS Message	Fan failure. Controller ‘’{0}’’.
Symptoms	None.
Severity	Critical
Category	Controller
Probable Causes	None.
Recommended Actions	None.

GUEST_USER_REMOVED

MIB Name	cLWAGuestUserRemoved
Alarm Condition	Guest user removed.
NCS Message	Guest user ‘’{1}’’ deleted on Controller ‘’{0}’’.
Symptoms	This notification is generated when the lifetime of the guest-user {1} expires and the guest-user's accounts are removed from Controller "{0}".
Severity	Informational
Category	Controller
Probable Causes	None.
Recommended Actions	None.

HEART_BEAT_LOSS

MIB Name	heartbeatLossTrap
Alarm Condition	Heart beat loss
NCS Message	Keepalive messages are lost between Master and Controller’’{0}’’.
Symptoms	None.
Severity	Major
Category	Controller
Probable Causes	None.
Recommended Actions	None.

IPSEC_ESP_AUTH_FAILURE

MIB Name	bsnIpsecEspAuthFailureTrap
Alarm Condition	IPsec ESP auth failure.
NCS Message	IPsec ESP Authentication failure from remote IP address ''{0}''. Error Count is ''{1}''.
Symptoms	None.
Severity	Minor
Category	Security
Probable Causes	None.
Recommended Actions	None.

IPSEC_ESP_INVALID_SPI

MIB Name	bsnIpsecEspInvalidSpiTrap
Alarm Condition	IPsec ESP invalid SPI
NCS Message	IPsec ESP Invalid SPI from remote IP address ''{0}''. IPsec SPI is ''{1}''.
Symptom	None.
Severity	Minor
Category	Security
Probable Causes	None.
Recommended Actions	None.

IPSEC_ESP_REPLAY_FAILURE

MIB Name	bsnIpsecEspReplayFailureTrap
Alarm Condition	IPsec ESP replay failure.
NCS Message	IPsec ESP Replay failure from remote IP address ''{0}''. Error Count is ''{1}''.
Symptoms	None.
Severity	Minor
Category	Security
Probable Causes	None.
Recommended Actions	None.

IPSEC_SUITE_NEG_FAILURE

MIB Name	bsnIpsecSuiteNegFailure
Alarm Condition	IPsec suite negotiation failure.
NCS Message	IPsec Suite Negotiation failure from remote IP address ''{0}''.
Symptoms	None.
Severity	Minor
Category	Security
Probable Causes	None.
Recommended Actions	None.

INVALID_RADIO

MIB Name	invalidRadioTrap
Alarm Condition	Invalid radio
NCS Message	Radio ''{0}'' with protocol ''{1}'' on controller ''{2}'' has invalid interface. ''{3}''
Symptoms	When the controller detects that a Cisco AP that has joined has unsupported radios, controller generates a trap and it gets propagated as an alert in the NCS.
Severity	Critical
Category	Access Point.
Probable Causes	None.
Recommended Actions	None.

LINK_FAILURE

MIB Name	linkFailureTrap
Alarm Condition	Link failure
NCS Message	Link failure. Controller ''{0}''.
Symptoms	None.
Severity	Critical
Category	Controller
Probable Causes	None.
Recommended Actions	None.

MESH_BATTERY

MIB Name	ciscoLwappMeshBatteryAlarm
Alarm Condition	Mesh Battery
NCS Message	MESH ''{0}'' battery status ''{1}''
Symptoms	None.
Severity	Critical
Category	Mesh Links
Probable Causes	None.
Recommended Actions	None.

MESH_DEFAULTBRIDGEGROUPNAME

MIB Name	ciscoLwappMeshDefaultBridgeGroupName
Alarm Condition	Mesh Default Bridge Group Name
NCS Message	MESH ''{0}'' has joined ''{1}'' with default bridge group name
Symptoms	None.
Severity	Major
Category	Mesh Links
Probable Causes	None.
Recommended Actions	None.

MESH_EXCESSIVECHILDREN

MIB Name	ciscoLwappMeshExcessiveChildren
Alarm Condition	Mesh Excessive Children
NCS Message	MESH ''{0}'' has exceeded child count of ''{1}'' for Mesh type ''{2}''.
Symptoms	
Severity	Major
Category	Mesh Links
Probable Causes	None.
Recommended Actions	None.

MESH_EXCESSIVEHOPCOUNT

MIB Name	ciscoLwappMeshExcessiveHopCount
Alarm Condition	Mesh Excessive Hop Count
NCS Message	MESH ''{0}'' number of hops from the MAP node to the RAP exceeds the threshold of ''{1}''
Symptoms	
Severity	Major
Category	Mesh Links
Probable Causes	None.
Recommended Actions	None.

MESH_QUEUEOVERFLOW

MIB Name	ciscoLwappMeshQueueOverflow
NCS Message	MESH ''{0}'' queue overflow peak packets ''{1}'' and packets dropped ''{2}''.
Symptoms	None.
Alarm Condition	Mesh Queue Pkt overflow
Severity	Critical
Category	Mesh Links
Probable Causes	None.
Recommended Actions	None.

MESH_SECBACKHAULCHANGE

MIB Name	ciscoLwappMeshSecBackhaulChange
Alarm Condition	Mesh Secondary Backhaul Change
NCS Message	MESH ''{0}'' changed backhaul from primary to secondary with ''{1}'' and backhaul is ''{2}'' with count ''{3}''.
Symptoms	None.
Severity	Major
Category	Mesh Links
Probable Causes	None.
Recommended Actions	None.

MSTREAM_CLIENT_DLIST

MIB Name	ciscoLwappMediaMCStreamDelistNotif
Alarm Condition	None.
NCS Message	Client ''{0}'' disconnected from the Media Stream with Reason code ''{1}''.
Symptoms	None.
Severity	Informational
Category	Clients
Probable Causes	None.
Recommended Actions	None.

MSTREAM_CLIENT_FAILURE

MIB Name	ciscoLwappMediaMCStreamFailureNotif
Alarm Condition	None.
NCS Message	Client ''{0}'' failed to get Media Stream with Reason code ''{1}''.
Symptoms	None.
Severity	Information
Category	Clients
Probable Causes	None.
Recommended Actions	None.

MSTREAM_CLIENT_ADMIT

MIB Name	ciscoLwappMediaMCStreamAdmitNotif
Alarm Condition	None.
NCS Message	Client ''{0}'' admitted to Media Stream.
Symptoms	None.
Severity	Informational
Category	Clients
Probable Causes	None.
Recommended Actions	None.

POWER_SUPPLY_CHANGE

MIB Name	powerSupplyStatusChangeTrap
Alarm Condition	Power supply change
Symptoms	None
Category	Controller
Severity	Critical
NCS Message	Power supply status changed. Controller ‘’{0}’’.
Probable Causes	None.
Recommended Actions	None.

RADAR_CHANNEL_DETECTED

MIB Name	bsnRadarChannelDetected
Alarm Condition	Radar channel detected
Symptoms	None.
Category	AP
Severity	Informational
NCS Message	Radar has been detected on channel ‘’{1}’’ by AP ‘’{0}’’ on 5GHz Radio.
Probable Causes	None.
Recommended Actions	None.

RADIOCARD_FAILURE

MIB Name	bsnAPRadioCardRxFailure
Alarm Condition	Radiocard failure.
Symptoms	None.
Category	AP
Severity	Critical

NCS Message	Depending on Receiver or Transmitter failure or clear it is one of the following: Transmitter failure detected on the "{0}" radio of AP "{1}" on Controller "{2}". Transmitter failure cleared on the "{0}" radio of AP "{1}" on Controller "{2}". Receiver failure detected on the "{0}" radio of AP "{1}" on Controller "{2}". Receiver failure cleared on the "{0}" radio of AP "{1}" on Controller "{2}".
Probable Causes	None.
Recommended Actions	None.

RADIO_CURRENT_TXPOWER_CHANGED

MIB Name	bsnAPCurrentTxPowerChanged
Alarm Condition	Radio transmit power level changed.
Symptoms	None.
Category	RRM
Severity	Informational.
NCS Message	Transmit Power changed to ‘’{2}’’ on ‘’{1}’’ interface of AP ‘’{0}’’ connected to Controller ‘’{3}’’.
Probable Causes	None.
Recommended Actions	None.

RRM_GROUPING_DONE

MIB Name	ciscoLwappRrmRfGroupLeaderChange
Alarm Condition	RRM grouping done.
Symptoms	None.
Category	RRM
Severity	Information
NCS Message	RF Group Leader changed for the ‘’{0}’’ network. New Group Leaders MAC address is ‘’{1}’’ IP address is ‘’{2}’’ Radio Type is ‘’{3}’’
Probable Causes	None.
Recommended Actions	None.

SIGNATURE_ATTACK

MIB Name	bsnSignatureAttackDetected
Alarm Condition	Signature attack
Symptoms	None.
Category	Security
Severity	Critical
NCS Message	IDS "{6}" Signature attack detected on AP "{0}" protocol "{3}" on Controller "{4}". The Signature description is "{7}", with precedence "{11}". The channel number is "{9}", the number of detections is "{10}", and one of potentially several attackers" mac addresses is "{8}".
Probable Causes	None.
Recommended Actions	None.

STATION_IOS_DEAUTHENTICATE

MIB Name	dot11Deauthenticate
Alarm Condition	Autonomous AP Client 802.1x authentication failure.
NCS Message	Client "{0}" is de-authenticated from AP "{1}" with reason code "{2}({3})".
Symptoms	This notification is generated by the AP when 802.1x authentication of the client fails.
Severity	Minor & Information (If the error code of the trap is > 13, then the alarms in generated with 'Minor' severity and under 'Security' category. If the error code is <= 12, then the event is generated with 'Information' severity under 'Client' category.).
Category	Clients and Security

Probable Causes	802.1x authentication failure of the client. Error Codes: 0 Reserved 1 Unspecified reason. 2 Previous authentication no longer valid. 3 Deauthenticated because sending station is leaving (or has left) IBSS or ESS. 4 Disassociated due to inactivity. 5 Disassociated because AP is unable to handle all currently associated stations. 6 Class 2 frame received from nonauthenticated station. 7 Class 3 frame received from nonassociated station. 8 Disassociated because sending station is leaving (or has left) BSS. 9 Station requesting (re)association is not authenticated with response. 11 Disassociated because the information in the Power Capability element is unacceptable. 12 Disassociated because the information in the Supported Channels element is unacceptable. 13 Invalid information element. 14 MIC failure 15 4-Way Handshake timeout. 16 Group Key Handshake timeout. 17 Information element in 4-Way Handshake different from (Re)Association Request/Probe. 18 Invalid group cipher. 19 Invalid pairwise cipher. 20 Invalid AKMP. 21 Unsupported RSN information element version. 22 Invalid RSN information element capabilities. 23 IEEE 802.1X authentication failed. 24 Cipher suite rejected per security policy.
Recommended Actions	Check client configuration for configured keys or passwords.

STATION_IOS_AUTHENTICATION_FAIL

MIB Name	dot11AuthenticateFail
Alarm Condition	Autonomous AP Client 802.11 authentication failure.
NCS Message	Client "{0}" has failed authenticating with AP "{1}". The reason code is "{2}({3})".

Symptoms	This notification is generated by the AP when 802.11 authentication of the client fails.
Severity	Informational.
Category	Clients
Probable Causes	802.11 Authentication failure of the client.
Recommended Actions	Check client configuration for configured keys or passwords.

STATION_WIRED_CHANGED

MIB Name	cmnMacChangedNotifications
Alarm Condition	MAC Address table notification trap.
NCS Message	Wired Client {0} {1} from Switch {2}
Symptoms	A MAC address table change on the switch.
Severity	Informational
Category	Clients.
Probable Causes	Switch detected a change in MAC address table.
Recommended Actions	None.

STP_NEWROOT

MIB Name	stpInstanceNewRootTrap.
Alarm Condition	STP newroot.
NCS Message	Controller "{0}". Spanning Tree Protocol Instance Root changed for VLAN ID "{1}".
Symptoms	This notification is generated by the AP when 802.11 authentication of the client fails.
Severity	Informational.
Category	Controller
Probable Causes	Failed Client authentication.
Recommended Actions	Check client configuration for configured keys or passwords.

TEMP_MOBILITY_ANCHOR_CTRL_PATH_DOWN

MIB Name	ciscoTempLwappMobilityAnchorControlPathDown
Alarm Condition	Mobility anchor control path down.

NCS Message	Controller ''{0}''. Control path on anchor ''{1}'' is down.
Symptoms	None.
Severity	Major
Category	Controller
Probable Causes	None.
Recommended Actions	None.

TEMP_MOBILITY_ANCHOR_DATA_PATH_DOWN

MIB Name	ciscoTempLwappMobilityAnchorDataPathDown
Alarm Condition	Mobility anchor data path down
NCS Message	Controller ''{0}''. Data path on anchor ''{1}'' is down.
Symptoms	None.
Severity	Major
Category	Controller
Probable Causes	None.
Recommended Actions	None.

TEMP_WLAN_ALL_ANCHORS_TRAP_DOWN

MIB Name	ciscoTempLwappMobilityAllAnchorsOnWlanDown
Alarm Condition	Mobility anchors down (Temp).
NCS Message	Controller ''{0}''. Data path on anchor ''{1}'' is down.
Symptoms	None.
Severity	Major
Category	Controller
Probable Causes	None.
Recommended Actions	None.

VOICE_COVERAGE_HOLE_ALARM

MIB Name	ciscoLwappDot11ClientCoverageHolePreAlarm
Alarm Condition	Voice coverage hole detected.
Symptoms	None.

Category	Coverage Hole
Severity	Information
NCS Message	Pre-Coverage Hole reported by "{0}" was found on Controller "{1}" near "{2}" with MacAddress "{3}".
Probable Causes	None.
Recommended Actions	None.

WLC_SCHEDULED_RESET

MIB Name	ciscoLwappScheduledResetNotif
Alarm Condition	None.
Symptoms	None.
Category	Controller
Severity	Informational
NCS Message	Controller ‘’{0}’’ is going to be reboot in {1} seconds.The reboot has been triggered from WLC command-line interface or Web Interface.
Probable Causes	None.
Recommended Actions	None.

Switch Traps

The following are the Switch traps added in the NCS 1.0:

COLD_START (FROM MIB-II STANDARD)

MIB Name	coldStart.
Alarm Condition	Cold start trap from controller.
NCS Message	Cold start. Switch "{0}."
Symptoms	The switch is reinitializing itself and that its configuration might have been altered.
Severity	Informational.
Category	Controller
Probable Causes	• The switch (controller) has power-cycled. • The switch (controller) went through a hard reset. • The switch (controller) went through a software restart.
Recommended Actions	Power recycled; Software reset.

LINK_DOWN (FROM MIB-II STANDARD)

MIB Name	linkDown.
Alarm Condition	Interface state change.
NCS Message	Port "{0}" is down on Switch "{1}."
Symptoms	The physical link on one of the switch (controller) ports is down.
Severity	Critical.
Category	Switch.
Probable Causes	A communication link to the port is disconnected.
Recommended Actions	None.

LINK_UP (FROM MIB-II STANDARD)

MIB Name	linkUp.
Alarm Condition	Interface state change.
NCS Message	Port "{0}" is up on Switch "{1}."
Symptoms	A previously down link on a switch port is up now.
Severity	Clear.
Category	Switch
Probable Causes	A communication link has been restored to the port.
Recommended Actions	None.

SWT_AUTH_FAIL

MIB Name	authenticationFailure
Alarm Condition	Authentication failed.
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch ‘’{0}’’. Authentication failed.
Probable Causes	None.
Recommended Actions	None.

SWT_CAEM_TEMPERATURE

MIB Name	caemTemperatureNotification
Alarm Condition	Over temperature Alarm Condition is detected in the managed system.

Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Over temperature Alarm Condition is detected in the managed system.
Probable Causes	None.
Recommended Actions	None.

SWT_CAEM_VOLTAGE

MIB Name	caemVoltageNotification
Alarm Condition	Over voltage Alarm Condition is detected in the managed system.
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch ''{0}''. Over voltage Alarm Condition is detected in the managed system.
Probable Causes	None.
Recommended Actions	None.

SWT_CDER_MON_EXCEPTION

MIB Name	cderMonitoredExceptionEvent
Alarm Condition	An exception is detected on the managed device.
Symptoms	None.
Category	Switch
Severity	Informational
NCS Message	Switch ''{0}''. An exception is detected on the managed device.
Probable Causes	None.
Recommended Actions	None.

SWT_CEFC_STATUS_CHANGE

MIB Name	cefcModuleStatusChange
Alarm Condition	CEFC Module status change.

Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	CEFC module state changed to ''{0}''. sysUpTime=''{1}''.
Probable Causes	None.
Recommended Actions	None.

SWT_CEV_FANONS15540_FAN_TRAY8

MIB Name	cevFanONS15540FanTray8
Alarm Condition	cevFanONS15540FanTray8 Notification.
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. cevFanONS15540FanTray8 Notification
Probable Causes	None.
Recommended Actions	None.

SWT_CEV_PORT_TRANSPARENT

MIB Name	cevPortTransparent
Alarm Condition	cevPortTransparent Notification
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. cevPortTransparent Notification
Probable Causes	None.
Recommended Actions	None.

SWT_CEV_PORT_WAVE

MIB Name	cevPortWave
Alarm Condition	cevPortWave Notification
Symptoms	None.

Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. cevPortWave Notification
Probable Causes	None.
Recommended Actions	None.

SWT_CONFIG_MAN_EVENT

MIB Name	ciscoConfigManEvent
Alarm Condition	Configuration management event has been recorded in ccmHistoryEventTable.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Configuration management event has been recorded in ccmHistoryEventTable.
Probable Causes	None.
Recommended Actions	None.

SWT_CONTENT_ENGINE_OVERLOAD

MIB Name	ciscoContentEngineOverloadBypass
Alarm Condition	A high watermark of percentage of capacity for transparent requests redirect.
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. A high watermark of percentage of capacity for transparent requests redirected to the Content Engine via WCCP (Web Cache Control Protocol) has been reached. Subsequent WCCP requests are rejected and forwarded to the Origin Server until the utilization falls below a low watermarker.
Probable Causes	None.
Recommended Actions	None.

SWT_CONTENT_ENGINE_WRITE_FAILED

MIB Name	ciscoContentEngineWriteTransFailed
Alarm Condition	Failed writing to working transaction log located in /local1/working.lo.
Symptoms	None.
Category	Switch
Severity	Critical
NCS Message	Switch ''{0}''. Failed writing to working transaction log located in /local1/working.lo
Probable Causes	None.
Recommended Actions	None.

SWT_CVPDN_SESSION

MIB Name	cvpdnNotifSession
Alarm Condition	L2X session with the indicated session ID and Xconnect VCID.
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. L2X session with the indicated session ID and Xconnect VCID.
Probable Causes	None.
Recommended Actions	None.

SWT_DMD_NBRLAYER2_CHANGE

MIB Name	demandNbrLayer2Change
Alarm Condition	D-Channel interface status change.
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	D-channel of interface ''{0}'' state changed to ''{1}''.
Probable Causes	None.
Recommended Actions	None.

SWT_ENV_MON_SHUTDOWN

MIB Name	ciscoEnvMonShutdownNotification
Alarm Condition	Environmental monitor detects a testpoint reaching a critical state.
NCS Message	Switch ''{0}''. Environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown.
Symptoms	None.
Severity	Informational.
Category	Switch
Probable Causes	None.
Recommended Actions	None.

SWT_GROUP_CHANGE

MIB Name	rptrGroupChange
Alarm Condition	Group structure of repeater has changed.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Group structure of repeater has changed.
Probable Causes	None.
Recommended Actions	None.

SWT_IP_PERMIT_DENIED

MIB Name	ipPermitDeniedTrap
Alarm Condition	None.
NCS Message	Switch "{0}". IP permit denied access.
Symptoms	None.
Severity	Informational.
Category	Switch
Probable Causes	None.
Recommended Actions	None.

SWT_LER_ALARM_ON

MIB Name	lerAlarmOn
Alarm Condition	None.
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch "{0}". LER has transitioned true state.
Probable Causes	None.
Recommended Actions	None.

SWT_LS1010_CHASSIS_CHANGE

MIB Name	ciscoLS1010ChassisChangeNotification
Alarm Condition	Cisco LS1010: Detected hot-swap component or changes in the chassis.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Cisco LS1010: Detected hot-swap component or changes in the chassis
Probable Causes	None.
Recommended Actions	None.

SWT_LS1010_CHASSIS_FAILURE

MIB Name	ciscoLS1010ChassisFailureNotification
Alarm Condition	Cisco LS1010: Change in the status of ps0 ps1 fan 12V line and/or chassis temperature.
Symptoms	None.
Category	Switch
Severity	Critical
NCS Message	Switch ''{0}''. Cisco LS1010: Change in the status of ps0 ps1 fan 12V line and/or chassis temperature.
Probable Causes	None.
Recommended Actions	None.

SWT_MODULE_DOWN

MIB Name	CISCO-STACK-MIB moduleDown
Alarm Condition	None.
NCS Message	Module "{0}" is down on Switch "{1}".
Symptoms	The module is changing state from OK.
Severity	Critical
Category	Switch
Probable Causes	None.
Recommended Actions	None.

SWT_MODULE_UP

MIB Name	CISCO-STACK-MIB moduleUp
Alarm Condition	None.
NCS Message	Module "{0}" is down on Switch "{1}".
Symptoms	The module is changing state from OK.
Severity	Clear
Category	Switch
Probable Causes	None.
Recommended Actions	None.

SWT_PETH_POWER_USAGE_OFF

MIB Name	pethMainPowerUsageOffNotification
Alarm Condition	PSE Threshold usage indication is off the usage power is below the threshold
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ‘’{0}’’. PSE Threshold usage indication is off the usage power is below the threshold.
Probable Causes	None.
Recommended Actions	None.

SWT_PETH_POWER_USAGE_ON

MIB Name	pethMainPowerUsageOnNotification
Alarm Condition	PSE Threshold usage indication is on the usage power is above the threshold.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. PSE Threshold usage indication is on the usage power is above the threshold.
Probable Causes	None.
Recommended Actions	None.

SWT_PETH_PSE_PORT_STATUS

MIB Name	pethPsePortDetectionStatus
Alarm Condition	The operational status of the port PD has changed.
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. The operational status of the port PD has changed.
Probable Causes	None.
Recommended Actions	None.

SWT_RESET_EVENT

MIB Name	rptrResetEvent
Alarm Condition	A repeater reset has completed.
Symptoms	None
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. A repeater reset has completed.
Probable Causes	None.
Recommended Actions	None.

SWT_RPTR_HEALTH

MIB Name	rptrHealth
Alarm Condition	Repeater (RPTR) status has changes or a non-disruptive test has completed
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch ''{0}''. Repeater (RPTR) status has changes or a non-disruptive test has completed.
Probable Causes	None.
Recommended Actions	None.

SWT_RTT_MON_CONN_CHANGE

MIB Name	rttMonConnectionChangeNotification
Alarm Condition	Connection to a target has either failed on establishment.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Connection to a target (not to a hop along the path to a target) has either failed on establishment or been lost and when reestablished.
Probable Causes	None.
Recommended Actions	None.

SWT_RTT_MON_NOTE

MIB Name	rttMonNotification
Alarm Condition	Threshold violation occurs during an operation to the target.
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. Threshold violation occurs during an operation to the target and not to a hop along the path to the target.
Probable Causes	None.
Recommended Actions	None.

SWT_RTT_MON_THRESHOLD

MIB Name	rttMonThresholdNotification
Alarm Condition	Threshold violation for an RTT operation occurred and subsided.
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. Threshold violation for an RTT operation occurred and subsided.
Probable Causes	None.
Recommended Actions	None.

SWT_RTT_MON_TIMEOUT

MIB Name	rttMonTimeoutNotification
Alarm Condition	Timeout for an RTT operation occurred and cleared.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Timeout for an RTT operation occurred and cleared.
Probable Causes	None.
Recommended Actions	None.

SWT_RTT_MON_VERIFY_ERROR

MIB Name	rttMonVerifyErrorNotification
Alarm Condition	Data corruption in an RTT operation has occurred.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Data corruption in an RTT operation has occurred.
Probable Causes	None.
Recommended Actions	None.

SWT_STP_NEW_ROOT

MIB Name	STPnewRoot
Alarm Condition	Sending agent has become the new root of the Spanning Tree.
Symptoms	None.
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. Sending agent has become the new root of the Spanning Tree
Probable Causes	None.
Recommended Actions	None.

SWT_STP_TOPOLOGY_CHANGE

MIB Name	STPtopologyChange
Alarm Condition	A port transitions from Learning state to Forwarding state.
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch ''{0}''. A port transitions from Learning state to Forwarding state or from Forwarding state to Blocking state.
Probable Causes	None.
Recommended Actions	None.

SWT_SWT_LER_ALARM_OFF

MIB Name	lerAlarmOff
Alarm Condition	None.
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch "{0}". LER has transitioned false state.
Probable Causes	None.
Recommended Actions	None.

SWT_SYS_CONFIG_CHANGE

MIB Name	sysConfigChangeTrap
Alarm Condition	System configuration in NVRAM is changed.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ‘’{0}’’. System configuration in NVRAM is changed
Probable Causes	None.
Recommended Actions	None.

SWT_VLAN_TRAUNK_PORT_DYN_STATUS

MIB Name	vlanTrunkPortDynamicStatusChange
Alarm Condition	The value of vlanTrunkPortDynamicStatus object has been changed.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ‘’{0}’’. The value of vlanTrunkPortDynamicStatus object has been changed.
Probable Causes	None.
Recommended Actions	None.

SWT_VM_VMPS_CHANGE

MIB Name	vmVmpsChange
Alarm Condition	Current VMPS has changed since the last system reinitialization.
Symptoms	None
Category	Switch
Severity	Major
NCS Message	Switch ''{0}''. Current VMPS has changed since the last system reinitialization. The current VMPS is changed whenever the VMPS fails to response after vmVmpsRetries of a VQP request.
Probable Causes	None.
Recommended Actions	None.

SWT_VTP_CONFIG_DIGEST_ERROR

MIB Name	vtpConfigDigestError
Alarm Condition	Configuration digest error occurred. The device received a VTP advertisement.
Symptoms	None
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Configuration digest error occurred. The device received a VTP advertisement.
Probable Causes	None.
Recommended Actions	None.

SWT_VTP_CONFIG_REV_NUMBER

MIB Name	vtpConfigRevNumberError
Alarm Condition	Configuration revision number error has occurred.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. Configuration revision number error has occurred.
Probable Causes	None.
Recommended Actions	None.

SWT_VTP_MTU_TOO_BIG

MIB Name	vtpMtuTooBig
Alarm Condition	The MTU size of the VLAN is larger than can be supported trunk ports
Symptoms	None
Category	Switch
Severity	Minor
NCS Message	Switch ''{0}''. The MTU size of the VLAN is larger than can be supported trunk ports.
Probable Causes	None.
Recommended Actions	None.

SWT_VTP_SERVER_DIABLED

MIB Name	vtpServerDisabled
Alarm Condition	Local server is no longer able to function as a VTP Server.
Symptoms	None
Category	Switch
Severity	Minor
NCS Message	Switch ''{0}''. Local server is no longer able to function as a VTP Server. The number of defined VLANs is greater than vtpMaxVlanStorage.
Probable Causes	None.
Recommended Actions	None.

SWT_VTP_VER1_DEV_DETECTED

MIB Name	vtpVersioNone.DeviceDetected
Alarm Condition	VTP version one device detected.
Symptoms	None.
Category	Switch
Severity	Information
NCS Message	Switch ''{0}''. VTP version one device detected that a management domain has been put into version 2 mode and 15 minutes has passed.
Probable Causes	None.
Recommended Actions	None.

SWT_VTP_VLAN_RING_NUM_CONFLICT

MIB Name	vtpVlanRingNumberConflict
Alarm Condition	Conflict between the ring number and the VTP-obtained ring number.
Symptoms	None.
Category	Switch
Severity	Minor
NCS Message	Switch ''{0}''. Conflict between the ring number and the VTP-obtained ring number.
Probable Causes	None.
Recommended Actions	None.

WARM_START

MIB Name	None.
Alarm Condition	Warm start trap from controller
NCS Message	Warm start. Switch "{0}".
Category	Switch
Symptoms	The switch is reinitializing itself such that its configuration is unaltered.
Severity	Informational
Probable Causes	Reboot was issued.
Recommended Actions	None.

Traps Added in the NCS Release 1.1

The following are the traps added for the NCS Release 1.1:

- FRIENDLY_ROGUE_AP_DETECTED_ON_NETWORK, page 13-120
- FRIENDLY_ROGUE_AP_DETECTED, page 13-120
- UNCLASSIFIED_ROGUE_AP_DETECTED_ON_NETWORK, page 13-121
- UNCLASSIFIED_ROGUE_AP_DETECTED_ON_NETWORK_AND_CONTAINED, page 13-121
- UNCLASSIFIED_ROGUE_AP_DETECTED_CONTAINED, page 13-122
- UNCLASSIFIED_ROGUE_AP_DETECTED, page 13-122
- MALICIOUS_ROGUE_AP_DETECTED_ON_NETWORK, page 13-123
- MALICIOUS_ROGUE_AP_DETECTED_ON_NETWORK_AND_CONTAINED, page 13-123
- MALICIOUS_ROGUE_AP_DETECTED_CONTAINED, page 13-124

FRIENDLY_ROGUE_AP_DETECTED_ON_NETWORK

MIB Name	bsnRogueAPDetected
Alarm Condition	Friendly Rogue AP detected on network.
Symptoms	A rogue access point was detected on network by the system with classification "Friendly".
Category	Rogue AP
Severity	Critical
NCS Message	Rogue AP "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Probable Causes	• An illegal access point has been connected to the network • A known internal or external access point unknown to this system has been detected as rogue.
Recommended Actions	• Verify the nature of the rogue access point by tracing it through the MAC address/SSID or by using location features to locate it physically. • If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within the NCS. • If the access point is deemed to be a security threat, the rogue can be contained using the management interface.

FRIENDLY_ROGUE_AP_DETECTED

MIB Name	bsnRogueAPDetected
Alarm Condition	Friendly Rogue AP detected.
Symptoms	A rogue access point was detected by the system with classification "Friendly".
Category	Rogue AP
Severity	Informational
NCS Message	Rogue AP "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".

Probable Causes	• An illegal access point has been connected to the system. • A known internal or external access point unknown to this system has been detected as rogue.
Recommended Actions	• Verify the nature of the rogue access point by tracing it through the MAC address/SSID or by using location features to locate it physically. • If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within the NCS. • If the access point is deemed to be a security threat, the rogue can be contained using the management interface.

UNCLASSIFIED_ROGUE_AP_DETECTED_ON_NETWORK

MIB Name	bsnRogueAPDetected
Alarm Condition	Unclassified Rogue AP detected on network.
Symptoms	A rogue access point was detected on network by the system with classification "Unclassified" in contained state.
Category	Rogue AP
Severity	Critical
NCS Message	Rogue AP "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Probable Causes	• An illegal access point has been connected to the network. • A known internal or external access point unknown to this system has been detected as rogue.
Recommended Actions	• Verify the nature of the rogue access point by tracing it through the MAC address/SSID or by using location features to locate it physically. • "If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within the NCS. • If the access point is deemed to be a security threat, the rogue can be contained using the management interface.

UNCLASSIFIED_ROGUE_AP_DETECTED_ON_NETWORK_AND_CONTAINED

MIB Name	bsnRogueAPDetected
Alarm Condition	Unclassified Rogue AP detected on network.
Symptoms	A rogue access point was detected on network by the system with classification "Unclassified" in contained state.
Category	Rogue AP
Severity	Major

NCS Message	Rogue AP "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Probable Causes	• An illegal access point has been connected to the network. • A known internal or external access point unknown to this system has been detected as rogue.
Recommended Actions	• Verify the nature of the rogue access point by tracing it through the MAC address/SSID or by using location features to locate it physically. • "If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within the NCS. • If the access point is deemed to be a security threat, the rogue can be contained using the management interface.

UNCLASSIFIED_ROGUE_AP_DETECTED_CONTAINED

MIB Name	bsnRogueAPDetected
Alarm Condition	Unclassified Rogue AP detected as contained.
Symptoms	A rogue access point was detected on network by the system with classification "Unclassified" in contained state.
Category	Rogue AP
Severity	Minor
NCS Message	Rogue AP "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Probable Causes	• An illegal access point has been connected to the network. • A known internal or external access point unknown to this system has been detected as rogue.
Recommended Actions	• Verify the nature of the rogue access point by tracing it through the MAC address/SSID or by using location features to locate it physically. • "If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within the NCS. • If the access point is deemed to be a security threat, the rogue can be contained using the management interface.

UNCLASSIFIED_ROGUE_AP_DETECTED

MIB Name	bsnRogueAPDetected
Alarm Condition	Unclassified Rogue AP detected.
Symptoms	A rogue access point was detected on network by the system with classification "Unclassified" in contained state.
Category	Rogue AP

Severity	Major.
NCS Message	Rogue AP "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Probable Causes	• An illegal access point has been connected to the network. • A known internal or external access point unknown to this system has been detected as rogue.
Recommended Actions	• Verify the nature of the rogue access point by tracing it through the MAC address/SSID or by using location features to locate it physically. • "If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within the NCS. • If the access point is deemed to be a security threat, the rogue can be contained using the management interface.

MALICIOUS_ROGUE_AP_DETECTED_ON_NETWORK

MIB Name	bsnRogueAPDetected
Alarm Condition	Malicious Rogue AP detected on network.
Symptoms	A rogue access point was detected on network by the system with classification "Malicious" in contained state.
Category	Rogue AP
Severity	Critical.
NCS Message	Rogue AP "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Probable Causes	• An illegal access point has been connected to the network. • A known internal or external access point unknown to this system has been detected as rogue.
Recommended Actions	• Verify the nature of the rogue access point by tracing it through the MAC address/SSID or by using location features to locate it physically. • "If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within the NCS. • If the access point is deemed to be a security threat, the rogue can be contained using the management interface.

MALICIOUS_ROGUE_AP_DETECTED_ON_NETWORK_AND_CONTAINED

MIB Name	bsnRogueAPDetected
Alarm Condition	Malicious Rogue AP detected on network and contained.
Symptoms	A rogue access point was detected on network by the system with classification "Malicious" in contained state.

Category	Rogue AP
Severity	Major.
NCS Message	Rogue AP "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Probable Causes	• An illegal access point has been connected to the network. • A known internal or external access point unknown to this system has been detected as rogue.
Recommended Actions	• Verify the nature of the rogue access point by tracing it through the MAC address/SSID or by using location features to locate it physically. • "If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within the NCS. • If the access point is deemed to be a security threat, the rogue can be contained using the management interface.

MALICIOUS_ROGUE_AP_DETECTED_CONTAINED

MIB Name	bsnRogueAPDetected
Alarm Condition	Malicious Rogue AP detected as contained.
Symptoms	A rogue access point was detected on network by the system with classification "Malicious" in contained state.
Category	Rogue AP
Severity	Minor.
NCS Message	Rogue AP "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Probable Causes	• An illegal access point has been connected to the network. • A known internal or external access point unknown to this system has been detected as rogue.
Recommended Actions	• Verify the nature of the rogue access point by tracing it through the MAC address/SSID or by using location features to locate it physically. • "If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within the NCS. • If the access point is deemed to be a security threat, the rogue can be contained using the management interface.

MALICIOUS_ROGUE_AP_DETECTED

MIB Name	bsnRogueAPDetected
Alarm Condition	Malicious Rogue AP detected.

Symptoms	A rogue access point was detected on network by the system with classification "Malicious" in contained state.
Category	Rogue AP
Severity	Major.
NCS Message	Rogue AP "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Probable Causes	• An illegal access point has been connected to the network. • A known internal or external access point unknown to this system has been detected as rogue.
Recommended Actions	• Verify the nature of the rogue access point by tracing it through the MAC address/SSID or by using location features to locate it physically. • "If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within the NCS. • If the access point is deemed to be a security threat, the rogue can be contained using the management interface.

MSE_HEALTH_MONITOR

MIB Name	None.
Alarm Condition	
Symptoms	This trap is generated on the NCS when a major event has occurred in the HA config. The alarm indicates to the user that status has changed and manual intervention might be required.
Category	Mobility Services
Severity	Critical (under the Mobility Services dashboard).
NCS Message	Depending on state of the Primary-Secondary pair different messages are sent to the NCS. Message sent include: Primary MSE <IP Address> is down. Manual failover configured. Administrator is required to invoke failover from the NCS. Primary MSE <IP Address> is down. Secondary cannot failover as the secondary is failing over for another primary server. Primary MSE <IP Address> lost connection to Secondary MSE. Primary MSE <IP Address> is down. Secondary MSE is taking over. Primary MSE server <IP Address> has reconnected with the secondary server. Secondary MSE server <IP Address> has reconnected with the primary server.
Probable Causes	• High availability state change.
Recommended Actions	• Manual intervention maybe required for events such as failover or failback configured for manual switching.

LICENSE_FILE_ALARM (MSE)

MIB Name	None.
Alarm Condition	
Symptoms	This trap is generated on the NCS when a major event has occurred in the HA config. The alarm indicates to the user that status has changed and manual intervention might be required.
Category	Mobility Services
Severity	Major (under the Mobility Services dashboard).
NCS Message	Depending on reason for rejecting a license file, the trap is sent in a XML format and is reflected in the NCS with the following alert messages: - <File Name> rejected. Ignoring license file for co-existence maximum limits - <File Name> rejected. Ignoring upgrade license file as corresponding base license is not installed - All service licenses rejected. Virtual Appliance needs to be first activated with a Virtual Appliance license. - <File Name> rejected. Ignoring license file as it is corrupt or could not be loaded.
Probable Causes	• Invalid or Corrupt license on MSE.
Recommended Actions	• Delete invalid or Corrupt license or fix the issue based on the alert message recommendation.

Alarms Raised Through Polling

This section lists those traps that are raised through polling and contains the following topics:

AP_DETECTED_DUPLICATE_IP

MIB Name	bsnDuplicateIpAddressReported.
Alarm Condition	AP Detected Duplicate IP.
NCS Message	AP "{0}" on Switch "{3}" detected duplicate IP address "{2}" being used by machine with mac address "{1}."
Symptoms	The system detects a duplicate IP address in the network that matches that assigned to an access point.
Severity	Critical.
Category	Security
Probable Causes	Another device in the network is configured with the same IP address as an access point.
Recommended Actions	Correct the misconfiguration of IP addresses in the network.

AUTHMGR-5-SUCCESS

MIB Name	AUTHMGR-5-SUCCESS
Alarm Condition	Wired client authorization success.
NCS Message	Authorization succeeded for client (%s) on Interface %s AuditSessionID %s
Symptoms	Authorization was successful.
Severity	Informational.
Category	Clients.
Probable Causes	Authorization was successful.
Recommended Actions	None.

AUTHMGR-5-FAIL

Syslog Name	AUTHMGR-5-FAIL
Alarm Condition	Wired client authorization failure.
NCS Message	Authorization failed or unapplied for client (%s) on Interface %s AuditSessionID %s
Symptoms	Authorization was unsuccessful.
Severity	Informational.
Category	Clients
Probable Causes	Authorization was unsuccessful.
Recommended Actions	None.

AUTHMGR-5-SECURITY_VIOLATION

Alarm Condition	Security violation on an Interface.
NCS Message	Security violation on the interface %s new MAC address (%e) is seen.AuditSessionID %s.
Symptoms	Security violation on an interface.
Category	Clients
Severity	Minor
Probable Causes	A host on the specified interface is attempting to gain access into the network or is trying to authenticate in a host mode that does not support the number of hosts attached. This is treated as a security violation and the port has been error-disabled.
Recommended Actions	Ensure that the port is configured to support the number of hosts attached. Enter the shutdown command followed by no shutdown command to restart the port.

DOT1X-5-SUCCESS

MIB Name	None.
Alarm Condition	Wired client 802.1X authentication success.
NCS Message	802.1X:Authentication was successful for client %s on Interface %s.
Symptoms	Authentication was successful.
Severity	Informational
Category	Clients
Probable Causes	Authentication was successful.
Recommended Actions	None.

DOT1X-5-FAIL

Alarm Condition	Wired client 802.1X authentication failure.
NCS Message	802.1X:Authentication failed for client %s on Interface %s.
Symptoms	Authentication was unsuccessful.
Severity	Informational
Category	Clients
Probable Causes	Authentication was unsuccessful.
Recommended Actions	None.

AP_DISASSOCIATED_MAINTENANCE

MIB Name	None.
Alarm Condition	None.
Category	Access Point.
Severity	Minor
NCS Message	AP "{0}" disassociated from Controller "{1}".
Probable Causes	None.
Recommended Actions	None.

CPM_UNREACHABLE

MIB Name	None.
Alarm Condition	Identity Services Engine down.
NCS Message	Identity Services Engine "{0}" is unreachable.
Symptoms	Identity Services Engine is not reachable by the NCS.
Severity	Major
Category	ISE
Probable Causes	Identity Services Engine is down or there is a network issue.
Recommended Actions	Check the status of Identity Services Engine.

IOSAP_ADMIN_DOWN

MIB Name	None.
Alarm Condition	Autonomous AP Admin Status Down

Category	Access Point.
Severity	Major
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

IOSAP_DOWN

MIB Name	None.
Alarm Condition	Autonomous AP Oper Status Down.
NCS Message	Autonomous AP "{0}" is unreachable.
Symptoms	The autonomous AP is SNMP unreachable.
Severity	Critical.
Category	Access Point.
Probable Causes	• Network connectivity to the autonomous access point is broken. • Ethernet port of the autonomous access point is down. • SNMP agent is not running in the autonomous access point. • SNMP credentials on the NCS do not match the SNMP credentials configured on the autonomous access point. • SNMP version on the NCS does not match the SNMP version configured on the autonomous access point.
Recommended Actions	First, check the IP connectivity to the access point. Next, check the port status of the access point. Finally, check SNMP credentials on both the NCS and the access point.

NCS_VERY_LOW_DISK_SPACE

MIB Name	None.
Alarm Condition	The NCS very low memory.
NCS Message	The NCS have very low disk space.
Symptoms	The NCS disk space meets requirement.
Severity	Critical.
Category	NCS
Probable Causes	Not enough disk space left on the NCS server.
Recommended Actions	Free some disk space.

NCS_LOW_MEMORY

MIB Name	None.
Alarm Condition	The NCS low memory.
NCS Message	The NCS has low memory.
Symptoms	The NCS server performance might be degrading.
Severity	Major.
Category	NCS
Probable Causes	The NCS has low memory.
Recommended Actions	Free up memory if possible.

NCS_CLIENT_TRAP_DISABLED

MIB Name	None.
Alarm Condition	Client Traps are disabled on controllers.
NCS Message	Client traps are disabled on controller(s) {0}.
Symptoms	This notification is generated by the NCS when required client traps are disabled in one or more controllers. These traps are needed for the NCS to detect client sessions in a timely and efficient manner. The required traps are: • 802.11 Association • 802.11 Disassociation • 802.11 Authentication • 802.11 Deauthentication • 802.11 Failed Association • 802.11 Failed Authentication
Severity	Minor.
Category	NCS
Probable Causes	When a controller is added to the NCS, the NCS enables the required client traps. If the NCS does not have the correct SNMP read-write community, it could fail. The trap controls can also be changed by pushing the SNMP trap control template or using controller graphical user interface or command-line interface.
Recommended Actions	Use the NCS template to enable the required client traps on the controller list.

AUTHMGR-5-START

MIB Name	None.
Alarm Condition	Start of wired client authentication.
NCS Message	Starting ‘%s’ for client (%s) on Interface %s AuditSessionID %s
Symptoms	Starting an authentication method.

Severity	Informational.
Category	Clients.
Probable Causes	Starting an authentication method.
Recommended Actions	None.

AUTHMGR-5-FAIL

MIB Name	None.
Alarm Condition	Wired client authorization failure.
Category	Clients
Symptoms	Authorization was unsuccessful.
Severity	Informational
NCS Message	Authorization failed or unapplied for client (%s) on Interface %s AuditSessionID %s.
Probable Causes	Authorization was unsuccessful.
Recommended Actions	None.

AUTHMGR-5-SECURITY_VIOLATION

MIB Name	None.
Alarm Condition	Security violation on an Interface.
Category	Clients
Symptoms	Security violation on an interface.
Severity	Minor
NCS Message	Security violation on the interface %s new MAC address (%e) is seen.AuditSessionID %s.
Probable Causes	A host on the specified interface is attempting to gain access into the network or is trying to authenticate in a host mode that does not support the number of hosts attached. This is treated as a security violation and the port has been error-disabled.
Recommended Actions	Ensure that the port is configured to support the number of hosts attached. Enter the shutdown command followed by no shutdown command to restart the port.

AUTHMGR-5-START

MIB Name	None.
Alarm Condition	Start of wired client authentication.

Category	Clients
Severity	Information
NCS Message	Starting 'mab' for client (%s) on Interface %s.
Probable Causes	None.
Recommended Actions	None.

AUTHMGR-5-SUCCESS

MIB Name	None.
Alarm Condition	Wired client authorization success.
Category	Clients
Severity	Informational.
NCS Message	Authorization succeeded for client (%s) on Interface %s AuditSessionID %s.
Probable Causes	None.
Recommended Actions	None.

AUTHMGR-SP-5-VLANASSIGN

MIB Name	None.
Alarm Condition	Wired Client critical VLAN assigned. Wired Client auth fail VLAN assigned. VLAN assignment as authorization policy. Wired Client guest VLAN assigned.
NCS Message	VLAN XXX assigned to Interface GiX/Y
Symptoms	VLAN assigned to an interface.
Severity	Informational
Category	Wired Clients
Probable Causes	VLAN assigned to an interface.
Recommended Actions	None.

APPLIANCE_FAN_BACK_TO_NORMAL

MIB Name	None.
Alarm Condition	Appliance fan error has cleared.

NCS Message	Fan is back to normal
Symptoms	A failure is no longer detected in the appliance fans.
Severity	Clear.
Category	NCS
Probable Causes	None.
Recommended Actions	None.

APPLIANCE_FAN_BAD_OR_MISSING

MIB Name	None.
Alarm Condition	A failure has been detected in the appliance fans.
NCS Message	Fan is either bad or missing.
Symptoms	A failure has been detected in the appliance fans.
Severity	Major.
Category	NCS
Probable Causes	A fan has failed.
Recommended Actions	Contact Technical Support.

APPLIANCE_POWER_SUPPLY_BACK_TO_NORMAL

MIB Name	None.
Alarm Condition	None.
NCS Message	Power supply is back to normal.
Symptoms	Power supply is back to normal.
Severity	Clear
Category	NCS
Probable Causes	None.
Recommended Actions	None.

APPLIANCE_POWER_SUPPLY_BAD_OR_MISSING

MIB Name	None.
Alarm Condition	None.
NCS Message	Power supply is either bad or missing.
Symptoms	Power supply is either bad or missing.
Severity	Major

Category	NCS
Probable Causes	Power supply is either bad or missing.
Recommended Actions	Replace bad or missing power supply.

APPLIANCE_RAID_BACK_TO_NORMAL

MIB Name	None.
Alarm Condition	None.
Symptoms	None.
Severity	Clear
NCS Message	RAID array in good health.
Category	Switch
Probable Causes	None.
Recommended Actions	None.

APPLIANCE_RAID_BAD_OR_MISSING

MIB Name	None.
Alarm Condition	None.
NCS Message	Drive "${0}" is missing or bad.
Symptoms	Disk or RAID failure.
Severity	Major
Category	NCS
Probable Causes	Disk or RAID failure.
Recommended Actions	Contact Technical Support. Replace failed drive.

APPLIANCE_TEMP_BACK_TO_NORMAL

MIB Name	None.
Alarm Condition	None.
NCS Message	Both CPU temperatures are OK.
Symptoms	None.
Severity	Clear
Category	Switch
Probable Causes	None.
Recommended Actions	None.

APPLIANCE_TEMP_EXCEED_UPPER_LIMIT

MIB Name	None.
Alarm Condition	None.
NCS Message	Appliance temperature exceeds upper limit.
Symptoms	None.
Severity	Major
Category	NCS
Probable Causes	None.
Recommended Actions	Contact Technical Support.

AUDIT_STATUS_DIFFERENCE

MIB Name	None.
Alarm Condition	Audit status difference.
NCS Message	Switch "{0}" Audit done at "(1)." Config differences found between the NCS and the controller.
Symptoms	This notification is generated by the NCS when audit differences are detected while auditing a controller during a network audit background task or per controller audit.
Severity	Minor.
Category	NCS
Probable Causes	The NCS and controller configuration are not synchronized.
Recommended Actions	Refresh the configuration from the controller so that it synchronizes with the controller configuration on the NCS.

CONFIG_BACKUP_FAILED

MIB Name	None.
Alarm Condition	Configuration backup failed.
Category	Controller
Severity	Warning
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

CONFIG_BACKUP_SUCCEEDED

MIB Name	None.
Alarm Condition	Configuration backup succeeded.
Category	Controller
Severity	Informational
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

COLD_START (FROM MIB-II STANDARD)

MIB Name	coldStart.
Alarm Condition	Cold start trap from controller.
NCS Message	Switch "{0}." Cold start.
Symptoms	The switch (controller) went through a reboot.
Severity	Informational.
Category	Controller
Probable Causes	• The switch (controller) has power-cycled. • The switch (controller) went through a hard reset. • The switch (controller) went through a software restart.
Recommended Actions	Power recycled; Software reset.

CONFIGAUDITSET_ENFORCEMENT_FAIL

MIB Name	None.
Alarm Condition	Enforcement on config group failed.
NCS Message	Failed to enforce Config Group “0” on controllers “1.”
Symptoms	This notification is generated by the NCS during network audit when some failures are encountered during enforcement of the templates from the config groups (which as opted to be enforced).
Severity	Critical.
Category	NCS
Probable Causes	The config group (which are opted to be enforced) templates are not in sync with the device values.
Recommended Actions	Look at the controller audit report for the list of enforced values and for the failed enforcements. An alarm is cleared upon successful enforcements during the next network audit cycle.

CONFIGAUDITSET_ENFORCEMENT_SUCCESS

MIB Name	None.
Alarm Condition	Enforcement on config group succeeded.
NCS Message	Successfully enforced Config Group “0” on controllers “1.”
Symptoms	This notification is generated by the NCS during network audit when all the templates from the config group (which are opted to be enforced) are successfully enforced.
Severity	Minor.
Category	NCS

Probable Causes	The config group (which are opted to be enforced) templates are not in sync with the device values.
Recommended Actions	Look at the controller audit report for the list of enforced values. An alarm is cleared when no enforcements are found during the next network audit cycle.

CONFIG_SAVED

MIB Name	bsnConfigSaved.
Alarm Condition	Configuration saved.
NCS Message	Switch "{0}." Configuration saved in flash.
Symptoms	A configuration save to flash is performed on the switch (controller).
Severity	Informational.
Category	Controller.
Probable Causes	The switch (controller) saves the configuration to the flash through a command-line interface command or entry via the controller graphical user interface or the NCS.
Recommended Actions	If you change the configuration using the controller command-line interface or controller graphical user interface, you might need to refresh the configuration.

CPM_REACHABLE

MIB Name	None.
Alarm Condition	Identity Services Engine reachable
NCS Message	Identity Services Engine "{0}" is reachable.
Symptoms	Identity Services Engine is reachable by the NCS.
Severity	Clear.
Category	ISE
Probable Causes	Clear alarm for CPM_UNREACHABLE.
Recommended Actions	None.

DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND

MIB Name	None.
Alarm Condition	Authorization vlan not found on switch.
NCS Message	Attempt to assign non-existent or shutdown VLAN %s to 802.1x port %s AuditSessionID %s
Symptoms	”An attempt was made to assign a VLAN to an 802.1x port but the VLAN was not found in the VTP database.”.

Severity	Informational
Category	Clients
Probable Causes	”An attempt was made to assign a VLAN to an 802.1x port but the VLAN was not found in the VTP database.”
Recommended Actions	Make sure the VLAN exists and is not shut-down or use another VLAN.

DOT1X-5-FAIL

MIB Name	None.
Alarm Condition	Wired client 802.1X authentication failure.
Category	Clients
Severity	Information
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

DOT1X-5-SUCCESS

MIB Name	None.
Alarm Condition	Wired client 802.1X authentication success.
Category	Clients
Severity	Information
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

DBADMIN_PASSWORD_RESET

MIB Name	None.
Alarm Condition	None.
NCS Message	DBAdmin password has been changed.
Symptoms	DBAdmin password has been changed.
Severity	Informational
Category	NCS

Probable Causes	Clear alarm for DBADMIN_PASSWORD_RESET_FAILED_ALERT.
Recommended Actions	None.

DBADMIN_PASSWORD_RESET_FAILED

MIB Name	None.
Alarm Condition	DBAdmin password reset failed.
NCS Message	DBAdmin password reset has failed.
Symptoms	DBAdmin password could not be reset.
Severity	Major
Category	NCS
Probable Causes	There is probably some issues with the database.
Recommended Actions	None.

DBADMIN_PASSWORD_RESET_FAILED_ALERTi

MIB Name	None.
Alarm Condition	None.
NCS Message	DBAdmin password reset failed.
Symptoms	DBAdmin password could not be reset.
Severity	Major
Category	NCS
Probable Causes	There is probably some issues with the database.
Recommended Actions	Contact system administrator.

EPM-4-POLICY_APP_FAILURE

MIB Name	None.
Alarm Condition	Failure in applying security policy for a wired client.
NCS Message	IP=%i| MAC=%e| AUDITSESID=%s| AUTHTYPE=%s| POLICY_TYPE=%s| POLICY_NAME=%s| RESULT=FAILURE| REASON=%s
Symptoms	The displayed policy for the client could not be applied by the policy enforcement module (PEM) for the reason indicated in the message.
Severity	Informational
Category	Clients

Probable Causes	The displayed policy for the client could not be applied by the Policy Enforcement Module (EPM) for the reason indicated in the message.
Recommended Actions	Take appropriate action based the failure reason indicated in the message.

EPM-6-POLICY_APP_SUCCESS

MIB Name	None.
Alarm Condition	Success in applying security policy for a wired client.
NCS Message	IP=%i| MAC=%e| AUDITSESID=%s| AUTHTYPE=%s| POLICY_TYPE=%s| POLICY_NAME=%s| RESULT=SUCCESS
Symptoms	The displayed policy for the client has been applied successfully by the EPM.
Severity	Informational/Clear
Category	Clients
Probable Causes	The displayed policy for the client has been applied successfully by the EPM.
Recommended Actions	None.

HM_CONFIGURATION

MIB Name	None.
Alarm Condition	The NCS failed HA configuration.
NCS Message	The NCS failed HA configuration.
Symptoms	The NCS failed on HA configuration.
Severity	Major
Category	NCS
Probable Causes	HA setup might be wrong.
Recommended Actions	Check HA setup.

HM_DATABASE_CRITICAL

MIB Name	ciscoWirelessMOStatusNotification
Alarm Condition	The NCS database is down.
NCS Message	Database is down, trying to restart.
Symptoms	The NCS database is down.
Severity	Critical
Category	NCS

Probable Causes	The database is down and cannot be started by HM.
Recommended Actions	Check server.

HM_DATABASE

MIB Name	ciscoWirelessMOStatusNotification
Alarm Condition	The NCS primary lost connection to the secondary.
NCS Message	The NCS lost connection with the other server.
Symptoms	The NCS lost connection with the other server.
Severity	Major
Category	NCS
Probable Causes	At the Database level, the connection between primary and secondary is lost. The server probably rebooted or shutdown.
Recommended Actions	Check server and network connections.

HM_FAILOVER

MIB Name	ciscoWirelessMOStatusNotification.
Alarm Condition	The NCS failover attempted and failed.
NCS Message	The NCS failover attempted and failed.
Symptoms	The NCS could not perform failover.
Severity	Major
Category	NCS
Probable Causes	Unknown.
Recommended Actions	Check server and network connections.

HM_FAILBACK

MIB Name	ciscoWirelessMOStatusNotification
Alarm Condition	The NCS failback attempted and failed.
NCS Message	The NCS failback attempted and failed.
Symptoms	The NCS could not perform failback.
Severity	Major
Category	NCS
Probable Causes	Unknown.
Recommended Actions	Check server and network connections.

HM_REACHABILITY

MIB Name	None.
Alarm Condition	The NCS primary and Secondary cannot reach each other.
NCS Message	The NCS servers cannot reach each other.
Symptoms	The NCS servers cannot reach each other.
Severity	Major
Category	NCS
Probable Causes	HA setup/configuration might be wrong. Servers might have also rebooted or shutdown.
Recommended Actions	Check HA setup/configuration.

HM_REGISTRATION

MIB Name	None.
Alarm Condition	The NCS failed HA registration.
NCS Message	The NCS failed HA registration.
Symptoms	The NCS failed on HA registration.
Severity	Major
Category	NCS
Probable Causes	HA configuration might be wrong.
Recommended Actions	Check HA configuration.

IOSAP_LINK_DOWN

MIB Name	linkDown
Alarm Condition	Autonomous AP Link Down.
NCS Message	Autonomous AP "{0}," Interface "{1}" is {2} down.
Symptoms	The physical link is down on an autonomous access point radio port.
Severity	Critical.
Category	Access Point.
Probable Causes	The radio port of an autonomous access point was disabled manually or a port failure occurred.
Recommended Actions	Check the administrative status of the port. If the port administrative status is not down, check other port settings.

IPSEC_ESP_POLICY_FAILURE

MIB Name	None.
Alarm Condition	IPsec ESP policy failure
Category	Security
Severity	Minor
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

IPSEC_OTHER_POLICY_FAILURE

MIB Name	None.
Alarm Condition	IPsec other policy failure
Category	Security
Severity	Minor
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

LICENSE_VIOLATION

MIB Name	None.
Alarm Condition	License violation
Category	NCS
Severity	Critical
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

LOC_SENSOR_UP

MIB Name	None.
Alarm Condition	None.

NCS Message	None.
Symptoms	
Severity	Minor
Category	None.
Probable Causes	None.
Recommended Actions	None.

LINK-3-UPDOWN

MIB Name	None.
Alarm Condition	Interface state change.
NCS Message	Interface %s, changed state to up/down.
Symptoms	None.
Severity	Informational
Category	Clients
Probable Causes	None.
Recommended Actions	None.

LOCATION_SENSOR_DOWN

MIB Name	None.
Alarm Condition	WiFi TDOA Receiver down
Category	Mobility Service
Symptoms	This alarm is generated when a TDOA Receiver is detected to be down by Aeroscout Engine running on MSE.
Severity	Minor
NCS Message	WiFi TDOA Receiver <MAC Address> <Name> is Down.
Probable Causes	TDOA Receiver is down.
Recommended Actions	Check if TDOA Receiver is physically down or contact Aeroscout support.

LOCATION_SERVER_DOWN

MIB Name	None.
Alarm Condition	MSE down
Category	Mobility Service

Severity	Critical
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

LOCATION_SERVER_LIMIT

MIB Name	None.
Alarm Condition	MSE limit reached
Category	Mobility Service
Severity	Major
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

LOCATION_SERVER_OUT_OF_SYNC

MIB Name	None.
Alarm Condition	Mobility Service out of sync.
Category	Mobility Service
Severity	Minor
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

LWAPP_AP_IF_DOWN_FC

MIB Name	None.
Alarm Condition	None.
Severity	Critical
NCS Message	None.
Category	Access Point.
Probable Causes	None.
Recommended Actions	None.

LWAPP_AP_IF_DOWN_RC

MIB Name	None.
Alarm Condition	None.
Severity	Informational.
NCS Message	None.
Category	Access Point.
Probable Causes	None.
Recommended Actions	None.

MSE_LICENSING

MIB Name	None.
Alarm Condition	MSE Licensing
Category	Mobility Service
Severity	Minor
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

MSE_NOTIFY

MIB Name	None.
Alarm Condition	MSE Notification
Category	Mobility Service
Severity	Information
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

MSE_UPGRADE

MIB Name	None.
Alarm Condition	MSE was upgraded from lower version.

Severity	Major
NCS Message	None.
Category	Mobility Service
Probable Causes	None.
Recommended Actions	None.

MAB-5-FAIL

MIB Name	None.
Alarm Condition	Wired client MAC authentication failure.
NCS Message	Authentication failed for client (%s) on Interface %s AuditSessionID %s
Symptoms	Authentication was unsuccessful.
Severity	Informational
Category	Clients.
Probable Causes	Authentication was unsuccessful.
Recommended Actions	None.

MAB-5-SUCCESS

Alarm Condition	Wired client MAC authentication success.
NCS Message	Authentication successful for client (%s) on Interface %s AuditSessionID.
Symptoms	Authentication was successful.
Severity	Informational
Category	Clients.
Probable Causes	Authentication was successful.
Recommended Actions	None.

NB_OSS_UNREACHABLE

MIB Name	None.
Alarm Condition	Northbound OSS server unreachable.
NCS Message	Northbound notification server "{0}" is unreachable. The NCS alarms are not processed for this server till it is reachable.
Symptoms	The NCS could not send notification through north bound.
Severity	Major
Category	Northbound

Probable Causes	Notification server might not be reachable.
Recommended Actions	Check the notification server.

NB_OSS_REACHABLE

MIB Name	None.
Alarm Condition	Northbound OSS server reachable.
NCS Message	Northbound notification server "{0}" is reachable.
Symptoms	The NCS could not send notification through north bound.
Severity	Major
Category	Northbound
Probable Causes	Notification server might not be reachable.
Recommended Actions	Check the notification server.

NCS_ALARM_TABLE_SIZE_BASED_CLEANUP_DONE

MIB Name	None.
Alarm Condition	Alarm table auto cleanup done.
NCS Message	Alarm table exceeds size limit.
Symptoms	Alarm table pruned.
Severity	Informational.
Category	NCS
Probable Causes	Alarm table exceeds size limit, the NCS performed a cleanup.
Recommended Actions	None.

NCS_DOWN

MIB Name	None.
Alarm Condition	The NCS Down
Category	NCS
Severity	Critical
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

NCS_EMAIL_FAILURE

MIB Name	None.
Alarm Condition	The NCS email failure.
NCS Message	The NCS with IP Address "{0}" failed to send e-mail.
Symptoms	This notification is generated by the NCS when it fails to send e-mails.
Severity	Major.
Category	NCS
Probable Causes	This can happen when SMTP server is either not configured or not reachable from the NCS.
Recommended Actions	Check Administration > Settings > Mail Server settings. Send a test e-mail from the mail server settings to see if it is successful.

NCS_NOTIFICATION_FAILURE

MIB Name	None.
Alarm Condition	The NCS notification failure.
NCS Message	The NCS with IP Address "{0}" failed to send notification. Please check Administration->Settings->Notification Receiver settings.
Symptoms	The NCS could not send notifications.
Severity	Major.
Category	NCS
Probable Causes	The notification destination not reachable.
Recommended Actions	Make Notification receiver configuration change.

NCS_LOW_DISK_SPACE

MIB Name	None.
Alarm Condition	The NCS has low disk space
NCS Message	The NCS “{0}” does not meet the minimum hardware requirements for disk space. Available: “{3}.” Minimum requirement: “{4}” Mb.
Symptoms	This notification is generated by the NCS when the free disk space where the NCS is installed does not meet minimum hardware requirements. This event is of major severity if minimum requirements are not met. This event is of critical severity when the available disk space is less than half of the minimum requirement.
Severity	Major/Critical.
Category	NCS
Probable Causes	This can happen when the disk is out of space.
Recommended Actions	Free up disk space.

NCS_OK_DISK_SPACE_BACKUP

MIB Name	None.
Alarm Condition	System has sufficient disk backup space.
NCS Message	The NCS "{0}" has sufficient disk space in directory "{1}" for backup. Space needed: "{2}"GB, space free: "{3}"GB”.
Symptoms	The NCS have enough disk space for backup.
Severity	Clear.
Category	NCS
Probable Causes	Clear alarm for the NCS_LOW_DISK_SPACE_BACKUP.
Recommended Actions	None.

NCS_OK_DISK_SPACE

MIB Name	None.
Alarm Condition	System has enough disk space.
NCS Message	The NCS "{0}" meets the minimum hardware requirements for disk space. Available: "{3}"GB. Minimum requirement: "{4}"GB.
Symptoms	The NCS disk space meets requirement.
Severity	Clear.
Category	NCS
Probable Causes	Clear alarm for the NCS_LOW_DISK_SPACE.
Recommended Actions	None.

NCS_LOW_DISK_SPACE_BACKUP

MIB Name	None.
Alarm Condition	The NCS does not have enough disk space for backup.
NCS Message	The NCS "{0}" does not have sufficient disk space in directory "{1}" for backup. Space needed: "{2}"GB, space free: "{3}"GB.
Symptoms	The NCS does not have enough disk space.
Severity	Major.
Category	NCS
Probable Causes	Disk space is low.
Recommended Actions	Free up disk space.

PASSWORD_EXPIRY_ALARM

MIB Name	None.
Alarm Condition	Root password expiry on MSE.
Category	Mobility Service
Severity	Warning
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

RADIO_COVERAGE_PROFILE_FAILED

MIB Name	bsnAPCoverageProfileFailed.
Alarm Condition	Radio coverage threshold violation.
NCS Message	AP "{0}," interface "{1}." Coverage threshold of "{3}" is violated. Total no. of clients is "{5}" and no. failed clients is "{4}."
Symptoms	Number of clients experiencing suboptimal performance has crossed the configured threshold.
Severity	Minor.
Category	Coverage Hole.
Probable Causes	Many clients are wandering to the remote parts of the coverage area of this radio interface with no handoff alternative.
Recommended Actions	• If the configured threshold is too low, you might need to readjust it to a more optimal value. • If the coverage profile occurs on a more frequent basis, you might need to provide additional radio coverage. • If the power level of this radio can be manually controlled, you might need to boost it to increase the coverage area.

RADIO_CURRENT_CHANNEL_CHANGED

MIB Name	bsnAPCurrentChannelChanged.
Alarm Condition	Radio current channel changed.
Symptoms	None.
Category	RRM
Severity	Informational
NCS Message	AP "{0}", interface "{1}". Channel changed to "{2}". Interference Energy before update was "{3}" and after update is "{4}".
Probable Causes	None.
Recommended Actions	None.

RADIO_INTERFERENCE_PROFILE_FAILED

MIB Name	None.
Alarm Condition	Radio interference threshold violation.
Severity	Minor
NCS Message	None.
Category	Access Point.

Probable Causes	None.
Recommended Actions	None.

RADIO_LOAD_PROFILE_FAILED

MIB Name	bsnAPLoadProfileFailed
Alarm Condition	Radio load threshold violation.
Symptoms	A radio interface of an Access point is reporting that the client load crossed a configured threshold.
Category	AP
Severity	Minor
NCS Message	AP "{0}", interface "{1}". Load threshold violated.
Probable Causes	There are too many clients associated with this radio interface.
Recommended Actions	• Verify the client count on this radio interface. If the threshold for this trap is too low, it might need to be readjusted • New capacity might need to be added to the physical location if the client count tends to be a frequent issue on this radio.

RADIO_NOISE_PROFILE_FAILED

MIB Name	bsnAPNoiseProfileFailed.
Alarm Condition	Radio noise threshold violation.
NCS Message	AP "{0}," interface "{1}." Noise threshold violated.
Symptoms	The monitored noise level on this radio has crossed the configured threshold.
Severity	Minor.
Category	Access Point.
Probable Causes	Noise sources that adversely affect the frequencies on which the radio interface operates.
Recommended Actions	• If the noise threshold is too low, you might need to readjust it to a more optimal value. • Investigate noise sources in the vicinity of the radio interface (for example, a microwave oven).

RADIO_SHUT_FAILED

MIB Name	None.
Alarm Condition	Radio shutdown failed.
NCS Message	Radio shutdown failed for AP “{0}” connected to controller “{1}.”
Symptoms	This notification is generated by the NCS during a scheduled operation for a given list of access point radios. It notifies the user that the status for certain radios has failed to change.
Severity	Major.
Category	Access Point.
Probable Causes	The controllers for the selected access point are not reachable, or the radio configurations are changed on the controller.
Recommended Actions	Check the NCS logs at the time of event generation and verify that the access point is associated with the controller.

RADIO_SHUT_SUCCESS

MIB Name	None.
Alarm Condition	Radio successfully shutdown.
NCS Message	Radio successfully shutdown for AP “{0}” connected to controller “{1}.”
Symptoms	This notification is generated by NCS during scheduled operation for a given list of access point radios. It notifies the user that the admin status has been successfully changed.
Severity	Informational.
Category	Access Point.
Probable Causes	None.
Recommended Actions	Verify the status of the specified radio on the controller.

RADIUS-4-RADIUS_ALIVE

Syslog Name	RADIUS-4-RADIUS_ALIVE
Alarm Condition	Radius server alive.
NCS Message	”RADIUS server [IP_address]:[int] [int] is being marked alive.”
Symptoms	A RADIUS server that previously was not responding has responded to a new request or the deadtimer has expired.
Severity	Minor
Category	Switch
Probable Causes	A RADIUS server that previously was not responding has responded to a new request or the dead timer has expired.
Recommended Actions	No action is required.

RADIUS-4-RADIUS_DEAD

MIB Name	None.
Alarm Condition	Radius server dead
Severity	Minor
NCS Message	RADIUS server %s is not responding.
Category	Switch
Probable Causes	Radius Server is not reachable from the NCS.
Recommended Actions	Check that Radius Server is reachable from the NCS.

ROGUE_ADHOC_DETECTED_ON_NETWORK

MIB Name	None.
Alarm Condition	Adhoc Rogue detected on network.
Category	Adhoc Rogue
Severity	Critical
NCS Message	Rogue AP "{0}" is on wired network.
Probable Causes	None.
Recommended Actions	None.

ROGUE_ADHOC_DETECTED_CONTAINED

MIB Name	None.
Alarm Condition	Adhoc Rogue detected contained.
Category	Adhoc Rogue
Severity	Minor
NCS Message	Rogue AP contained.
Probable Causes	Manual or auto containment action.
Recommended Actions	None.

ROGUE_AP_STATE_CHANGE

MIB Name	None.
Alarm Condition	Rogue detected.
Category	Rogue AP.
Severity	Minor
NCS Message	Rogue AP marked as {0} AP.
Probable Causes	User action.
Recommended Actions	None.

ROGUE_DETECTED

MIB Name	None.
Alarm Condition	Rogue detected.
NCS Message	:Rogue AP "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Severity	Minor
Category	Rogue AP
Probable Causes	None.
Recommended Actions	None.

ROGUE_DETECTED_CONTAINED

MIB Name	None.
Alarm Condition	Rogue detected contained.
Category	Rogue AP
Severity	Minor
NCS Message	Adhoc Rogue contained.
Probable Causes	Manual or auto containment action.
Recommended Actions	None.

ROGUE_DETECTED_ON_NETWORK

MIB Name	None.
Alarm Condition	Rogue detected on network.
Category	Rogue AP
Severity	Critical
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

ROGUE_AUTO_CONTAINED

MIB Name	None.
Alarm Condition	Rogue auto contained.
Category	Security
Severity	Major
NCS Message	Rogue AP "{0}" on Controller "{1}" was advertising our SSID and has been auto contained as per WPS policy.
Probable Causes	None.
Recommended Actions	None.

SWITCH_DOWN

MIB Name	This is a NCS-only event.
Alarm Condition	Controller down.
NCS Message	Switch "{0}" is unreachable.
Symptoms	A switch (controller) is unreachable from the management system.
Severity	Critical.
Category	Controller
Probable Causes	• The switch (controller) has encountered hardware or software failure. • There are network connectivity issues between the management station and the switch (controller). • The configured SNMP community strings on the management station or the switch (controller) are incorrect.
Recommended Actions	• Check if the switch (controller) is powered up and reachable through the web interface. • Ping the switch (controller) from the management station to verify if there is IP connectivity. • Check the community strings configured on the management station.

SWT_SWITCH_DOWN

MIB Name	None.
Alarm Condition	Switch down
Category	Switch
Severity	Critical
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

STATION_AUTHFAIL_VLAN_ASSIGNED

MIB Name	None.
Alarm Condition	Wired Client auth fail VLAN assigned
Category	Clients
Severity	Information
NCS Message	None.

Probable Causes	None.
Recommended Actions	None.

STATION_CRITICAL_VLAN_ASSIGNED

MIB Name	None.
Alarm Condition	Wired Client critical VLAN assigned
Category	Clients
Severity	Information
NCS Message	Critical VLAN %s is assigned to Wired Client "%s".
Probable Causes	Radius Server is not reachable from the Access Switch.
Recommended Actions	Check that Radius Server is reachable from Access Switch.

STATION_GUEST_VLAN_ASSIGNED

MIB Name	None.
Alarm Condition	Wired Client guest VLAN assigned
Category	Clients
Severity	Information
NCS Message	Guest VLAN %s is assigned to Wired Client '%s".
Probable Causes	Client is moved to Auth Fail VLAN because client failed authentication.
Recommended Actions	Check that client provided appropriate credentials.

TRACKED_CLIENT_DETECTION

MIB Name	None.
Alarm Condition	Tracked client detected on the network.
Category	Security
Severity	Major
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

USER_AUTHENTICATION_FAILURE

MIB Name	None.
Alarm Condition	User Authentication Failure.
Category	Security
Severity	Informational
NCS Message	"%s" "%s" failed authentication on Controller "%s".
Probable Causes	User failed to authenticate.
Recommended Actions	Check that user provides appropriate credentials.

WARM_START

MIB Name	None.
Alarm Condition	Warm start trap from controller
Category	Controller
Severity	Informational
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

Wireless Intrusion Protection Alarms

MIB Name	None.
Alarm Condition	wIPS engine on MSE.
NCS Message	Dynamically generated. Refer NCS Monitor > Alarms.
Symptoms	Refer to wIPS alarm encyclopedia under NCS > Configuration > wIPS Profiles.
Severity	Critical.
Category	Mobility Service
Probable Causes	Possible security attack.
Recommended Actions	None.

WLAN_SHUT_FAILED

MIB Name	None.
Alarm Condition	Client associated failure with AP.
NCS Message	Wlan "{0}" shutdown failed on controller "{1}."
Symptoms	This notification is generated by the NCS during scheduled operations for a given WLAN Config object. It notifies the user that the WLAN status did not change at the scheduled time.
Severity	Major.
Category	NCS
Probable Causes	The controller for the selected WLAN is not reachable, or the WLAN object does not exist.
Recommended Actions	Check the NCS logs at the time of event generation and verify if the WLAN exists on the controller.

WLAN_SHUT_SUCCESS

MIB Name	None.
Alarm Condition	WLAN successfully shutdown.
NCS Message	Wlan "{0}" successfully shutdown on controller "{1}."
Symptoms	This notification is generated by the NCS during scheduled operation for each given WLAN configuration object. It notifies the user that the admin status has been successfully completed.
Severity	Informational.
Category	NCS
Probable Causes	Verify the admin status for the displayed WLAN on the controller.
Recommended Actions	Remove the event from the event list page.

WLC_CANCEL_SCHEDULED_RESET

MIB Name	None.
Alarm Condition	None.
Category	Controller
Severity	Informational
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

WLC_SCHEDULED_RESET_FAILED

MIB Name	None.
Alarm Condition	None.
Category	Controller
Severity	Information
NCS Message	None.
Probable Causes	None.
Recommended Actions	None.

Unsupported Traps

- BROADCAST_STORM_START: broadcastStormStartTrap
- FAN_FAILURE: fanFailureTrap
- POWER_SUPPLY_STATUS_CHANGE: powerSupplyStatusChangeTrap
- BROADCAST_STORM_END: broadcastStormEndTrap
- VLAN_REQUEST_FAILURE: vlanRequestFailureTrap
- VLAN_DELETE_LAST: vlanDeleteLastTrap
- VLAN_DEFAULT_CFG_FAILURE: vlanDefaultCfgFailureTrap
- VLAN_RESTORE_FAILURE_TRAP: vlanRestoreFailureTrap
- IPSEC_ESP_REPLAY_FAILURE: bsnIpsecEspReplayFailureTrap
- IPSEC_ESP_INVALID_SPI: bsnIpsecEspInvalidSpiTrap
- LRAD_UP: bsnAPUp
- LRAD_DOWN: bsnAPDown
- STP_NEWROOT: stpInstanceNewRootTrap
- STP_TOPOLOGY_CHANGE: stpInstanceTopologyChangeTrap
- BSN_DOT11_ESS_CREATED: bsnDot11EssCreated
- BSN_DOT11_ESS_DELETED BSNDOT11ESSDELETED
- LRADIF_RTS_THRESHOLD_CHANGED
- LRADIF_ED_THRESHOLD_CHANGED
- LRADIF_FRAGMENTATION_THRESHOLD_CHANGED
- LINK_FAILURE: linkFailureTrap

CHAPTER 14

Reports

The Cisco NCS reporting is necessary to monitor the system and network health as well as troubleshoot problems. A number of reports can be generated to run on an immediate and scheduled basis. Each report type has a number of user-defined criteria to aid in the defining of the reports. The reports are formatted as a summary, tabular, or combined (tabular and graphical) layout. Once defined, the reports can be saved for future diagnostic use or scheduled to run and report on a regular basis.

Reports are saved in either CSV or PDF format and are either saved to a file on the NCS for later download or e-mailed to a specific e-mail address.

The reporting types include the following:

- Current, which provides a snap shot of the data that is not dependent upon time.
- Historical, which retrieves data from the device periodically and stores it in the NCS database
- Trend, which generates a report using aggregated data. Data can be periodically collected based from devices on user-defined intervals, and a schedule can be established for report generation.

With the NCS, you also have the ability to export any report that you can view, sort reports into logical groups, and archive for long-term storage.

Note As of the NCS 1.x, the size limitations for reports is removed. So, you can view a report of any size with any number of graphs using HTML or saved as CSV/PDF files.

The Reports menu provides access to all the NCS reports as well as currently saved and scheduled reports.

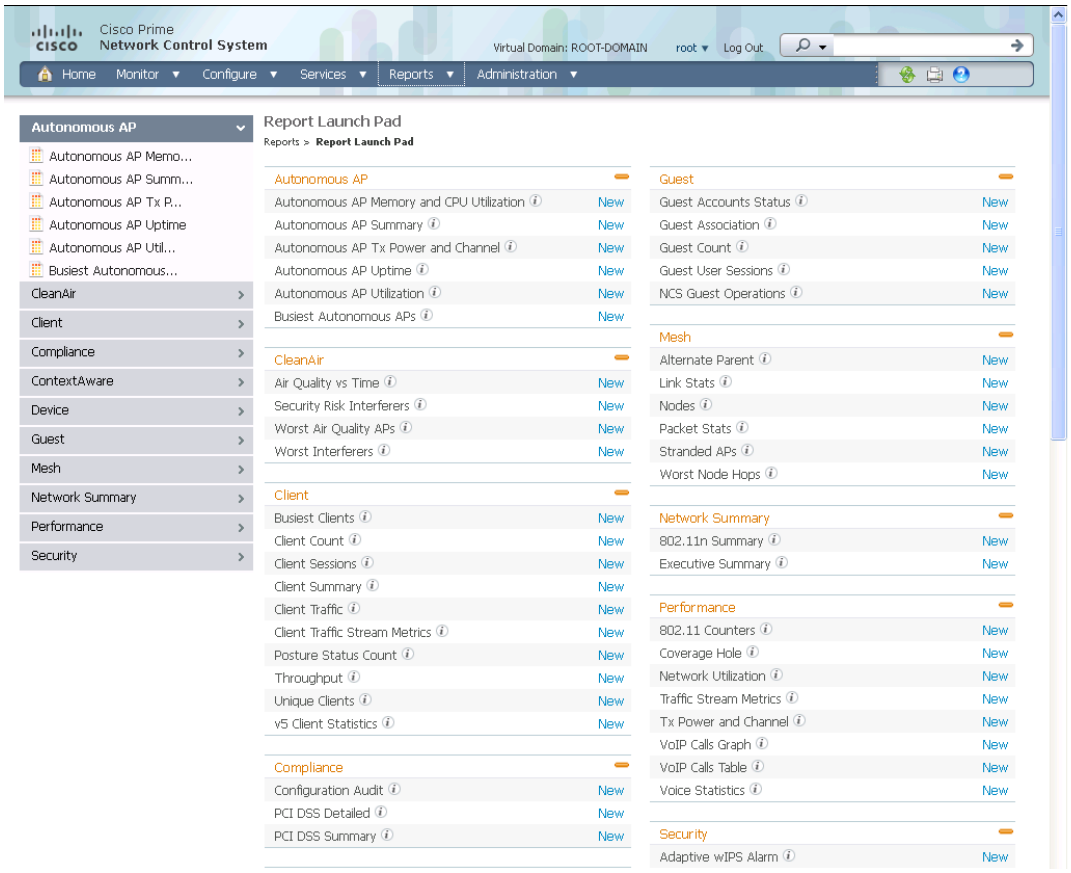
- Report Launch Pad—The hub for all the NCS reports. From this page, you can access specific types of reports and create new reports. See the "Report Launch Pad" section on page 14-2 for more information.
- Scheduled Run Results—Allows you to access and manage all currently scheduled runs in the NCS. In addition, allows you to access and manage on-demand export as well as e-mailed reports. See the "Managing Scheduled Run Results" section on page 14-15 for more information.
- Saved Report Templates—Allows you to access and manage all currently saved report templates in the NCS. See the "Managing Saved Report Templates" section on page 14-17 for more information.

Report Launch Pad

The report launch pad provides access to all the NCS reports from a single page. From this page, you can view current reports, open specific types of reports, create and save new reports, and manage scheduled runs (see Figure 14-1).

Tip Hover your mouse cursor over the tool tip next to the report type to view more report details.

Figure 14-1 Report Launch Pad



This section contains the following topics:

- Mapping Reports in the WCS with Reports in the NCS, page 14-3
- Creating and Running a New Report, page 14-6
- Managing Current Reports, page 14-14
- Managing Scheduled Run Results, page 14-15
- Managing Saved Report Templates, page 14-17

Mapping Reports in the WCS with Reports in the NCS

Table 14-1 provides the mapping between the reports in WCS and reports in the NCS. Additionally, the new reports that were added to the NCS are also specified.

Table 14-1 Mapping Reports in WCS with Reports in the NCS

Reports	In WCS	In NCS
Autonomous AP	-	-
Autonomous AP Memory and CPU Utilization	No	Yes
Autonomous AP Summary	No	Yes
Autonomous AP Tx Power and Channel	No	Yes
Autonomous AP Uptime	No	Yes
Autonomous AP Utilization	No	Yes
Busiest Autonomous APs	No	Yes
CleanAir	-	-
Air Quality vs Time	Yes	Yes
Security Risk Interferers	Yes	Yes
Worst Air Quality APs	Yes	Yes
Worst Interferers	Yes	Yes
Client	-	-
Busiest Clients	Yes	Yes
Client Count	Yes	Yes
Client Sessions	Yes	Yes
Client Summary	Yes	Yes
Client Traffic	Yes	Yes
Client Traffic Stream Metrics	Yes	Yes
Posture Status Count	No	Yes
Throughput	Yes	Yes
Unique Clients	Yes	Yes
CCX Client Statistics	Yes	Yes
Compliance	-	-
Configuration Audit	Yes	Yes
PCI DSS Detailed	Yes	Yes
PCI DSS Summary	Yes	Yes
ContextAware	-	-
Client Location History	Yes	Yes
Client Location Tracking	Yes	Yes

Table 14-1 Mapping Reports in WCS with Reports in the NCS (continued)

Reports	In WCS	In NCS
Guest Location Tracking	Yes	Yes
Location Notifications	Yes	Yes
Rogue AP Location Tracking	Yes	Yes
Rogue Client Location Tracking	Yes	Yes
Tag Location History	Yes	Yes
Tag Location Tracking	Yes	Yes
Device	-	-
AP Image Pre-download	Yes	Yes
AP Profile Status	Yes	Yes
AP Summary	Yes	Yes
Busiest APs	Yes	Yes
CPU Utilization	Yes	Yes
Detailed Switch Inventory	No	Yes
Identity Capability	No	Yes
Inventory	No	Yes
Memory Utilization	Yes	Yes
Non-Primary Controller APs	No	Yes
Switch Interface Utilization	No	Yes
Up Time	Yes	Yes
Utilization	Yes	Yes
Guest	-	-
Guest Accounts Status	Yes	Yes
Guest Association	Yes	Yes
Guest Count	Yes	Yes
Guest User Sessions	Yes	Yes
NCS Guest Operations	Yes	Yes
MSAP	--	--
Mobile MAC Statistics	No	Yes
Service URI Statistics	No	Yes
Identity Services Engine	--	--
Posture Detail Assessment	No	Yes
Endpoint Profiler Summary	No	Yes
Top N Endpoint MAC Authentications	No	Yes
Endpoint MAC Authentication Summary	No	Yes
User Authentication Summary	No	Yes

Table 14-1 Mapping Reports in WCS with Reports in the NCS (continued)

Reports	In WCS	In NCS
Top N User Authentications	No	Yes
Radius Accounting	No	Yes
Radius Authentication	No	Yes
Mesh	-	-
Alternate Parent	Yes	Yes
Link Stats	Yes	Yes
Nodes	Yes	Yes
Packet Stats	Yes	Yes
Stranded APs	Yes	Yes
Worst Node Hops	Yes	Yes
Network Summary	Yes	Yes
802.11n Summary	Yes	Yes
Executive Summary	Yes	Yes
Preferred Calls Report	Yes	Yes From the NCS 1.1 onwards.
Performance	-	-
802.11 Counters	Yes	Yes
Coverage Hole	Yes	Yes
Network Utilization	Yes	Yes
Traffic Stream Metrics	Yes	Yes
Tx Power and Channel	Yes	Yes
VoIP Calls Graph	Yes	Yes
VoIP Calls Table	Yes	Yes
Voice Statistics	Yes	Yes
Security	-	-
Adaptive wIPS Alarm	Yes	Yes
Adaptive wIPS Alarm Summary	Yes	Yes
Adaptive wIPS Top 10 AP	Yes	Yes
Adhoc Rogue Count Summary	Yes	Yes
Adhoc Rogues	Yes	Yes
New Rogue AP Count Summary	Yes	Yes
New Rogue APs	Yes	Yes
Rogue AP Count Summary	Yes	Yes
Rogue APs	Yes	Yes
Security Alarm Trending Summary	Yes	Yes

Non Upgradable Reports from the WCS to the NCS

The following reports cannot be upgraded to the NCS 1.0 and later:

- Adhoc Rogue Count Summary
- Adhoc Rogues
- Client Count
- Client Summary
- Client Throughput
- New Rogue AP Count Summary
- New Rogue APs
- Rogue AP Count Summary
- Rogue APs
- Security Alarm Trending Summary

Note You cannot upgrade the Guest User Sessions reports to the NCS Release 1.1.

Creating and Running a New Report

To create and run a new report, follow these steps:

Step 1 Choose **Reports > Report Launch Pad**.

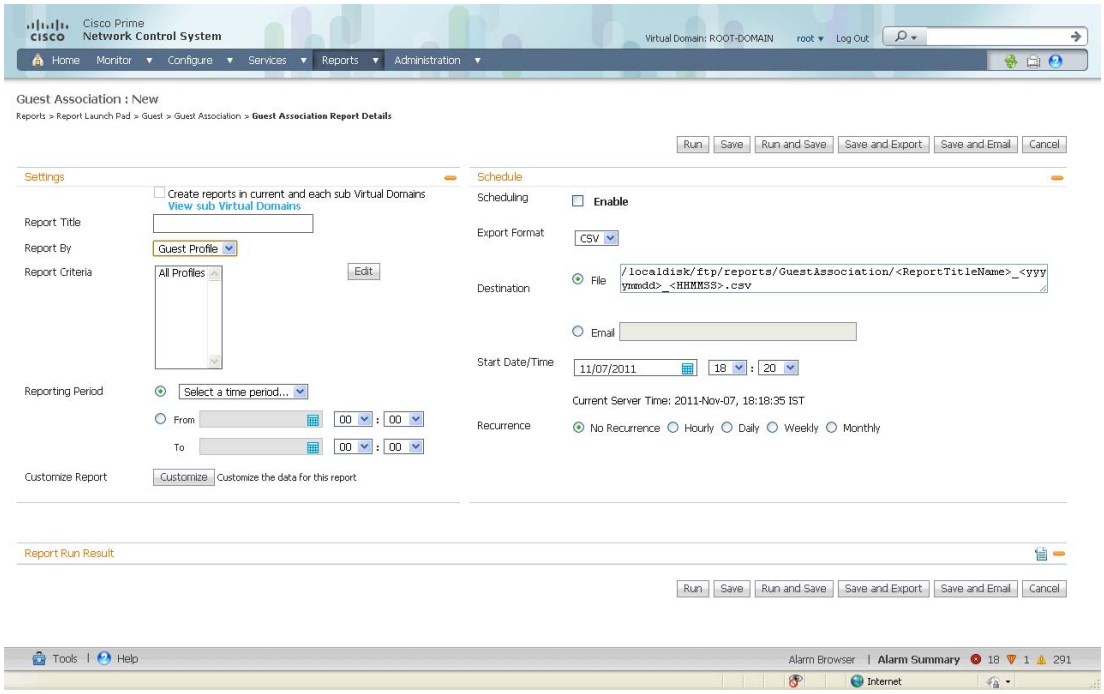
The reports are listed by category in the main section of the page and on the left sidebar menu (see Figure 14-1).

Step 2 Find the appropriate report in the main section of the Report Launch Pad.

Note Click the report name from the Report Launch Pad or use the navigation on the left side of the Report Launch Pad page to view any currently saved report templates for that report type.

Step 3 Click **New** to the right of the report. The Report Details page appears (see Figure 14-2).

Figure 14-2 Report Details Page



Step 4 In the Report Details page, enter the following Settings parameters:

Note Certain parameters might or might not appear depending on the report type.

- Create reports in current and each sub Virtual Domains—Select this check box if you want to create reports not only in current virtual domain but also for each sub virtual domains. Click the View applied Virtual Domains link to view details about the virtual domains such as the name of the virtual domain, e-mail address and the time zone.

Note If this check box is enabled and the report is not scheduled, the report template is created and saved in all the subdomains but the report is not run. But if the Create reports in current and sub Virtual Domains check box is checked, and the report is scheduled, then the report is scheduled in all the subdomains and is run at the scheduled time.

Note If this check box is enabled, you can only save the report and therefore all other options such as run, run and save, save and export, save and e-mail are not visible in the report details page. This means that the reports can only be created and scheduled to run in sub domains.

Note There should be sufficient time interval (at least 30 minutes) between the report creation and report execution as the report creation time varies between different systems.

- Report Title—If you plan to use this as a saved report template, enter a report name.

  Note This report title is suffixed with *_VirtualDomainName* if you select the Create reports in current and each sub Virtual Domains check box. The *VirtualDomainName* is the name of the virtual domain for which the report has been generated.

- Report By—Choose the appropriate Report By category from the drop-down list. The categories differ for each report. See specific report sections for Report By categories for each report.
- Report Criteria—The field allows you to sort your results depending on the previous Report By selection made. Click **Edit** to open the Filter Criteria page.

  Note Click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Connection Protocol—Choose either of these protocols **All Clients**, **All Wired (802.3)**, **All Wireless (802.11)**, **802.11a/n**, **802.11b/g/n**, **802.11a**, **802.11b**, **802.11g**, **802.11n (5 GHz)**, or **802.11n (2.4 GHz)**.
- SSID—All SSIDs is the default value.
- Report Period
  - Last—Select the **Last** radio button and choose the period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed in the report.

  Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Step 5 If you plan to run this report at a later time or as a recurring report, enter the Schedule parameters. The Schedule parameters allow you to control when and how often the report runs.

- Enable Schedule—Select the check box to run the report on the set schedule.
- Export Format—Choose your format for exported files (CSV or PDF).

  Note The default file locations for CSV and PDF files are as follows:

  /ncs-ftp/reports/Inventory/*ReportTitleName_yyyymmdd_HHMMSS.csv*
  /ncs-ftp/reports/Inventory/*ReportTitleName_yyyymmdd_HHMMSS.pdf*

- Destination—Choose your destination type (File or Email). Enter the applicable file location or the e-mail address.

  If you selected Create reports in current and each sub Virtual Domains check box then the Email to default Contact in each Virtual Domain radio button appears instead of the Email radio button. You can click the **View Contacts** link to view the e-mail IDs for the various virtual domains.

Note To set the mail server setup for e-mails, choose **Administration > Settings**, then choose **Mail Server** from the left sidebar menu to open the Mail Server Configuration page. Enter the SMTP and other required information.

Note If an e-mail address is not specified for a subVirtual Domain then the e-mail address of the current Virtual Domain is used if it is specified for the current Virtual Domain.

- Start Date/Time—Enter a date in the provided text box or click the **calendar** icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists. The report begins to run on this data and at this time.

  Note The time referred here is the NCS server time and not the local time of the browser.

  Note If you selected Create reports in current and each sub Virtual Domains check box then the Use Virtual Domain time zone check box appears. Select this check box if you want to use the time zone of the virtual domain as the time zone. Click the **View time zones** link to view the timezones of the various virtual domains.

- Recurrence—Enter the frequency of this report.
  - No Recurrence—The report runs only once (at the time indicated for the Start Date/Time).
  - Hourly—The report runs on the interval indicated by the number of hours you enter in the Entry text box.
  - Daily—The report runs on the interval indicated by the number of days you enter in the Every text box.
  - Weekly—The report runs on the interval indicated by the number of weeks you enter in the Every text box and on the days specified by the selected check boxes.

The Create Custom Report page allows you to customize the report results. Table 14-2 specifies which reports are customizable, which have multiple subreports, and which report views are available. In future releases, all reports will be customizable.

Table 14-2 Report Customization

Report	Customizable?	Multiple SubReports?	Report Views	Data Field Sorting?
Autonomous AP Memory and CPU Utilization	No	No	Graphical	No
Autonomous AP Summary	Yes	No	Tabular	No
Autonomous AP Tx Power and Channel	No	Yes	Graphical	No

Table 14-2 Report Customization (continued)

Report	Customizable?	Multiple SubReports?	Report Views	Data Field Sorting?
Autonomous AP Uptime	Yes	No	Tabular	No
Autonomous AP Utilization	No	No	Graphical	No
Busiest Autonomous APs	Yes	No	Tabular	No
Air Quality vs Time	Yes	No	Tabular	No
Security Risk Interferers	Yes	No	Tabular	No
Worst Air Quality APs	Yes	No	Tabular	No
Worst Interferers	Yes	No	Tabular	No
Busiest Clients	Yes	No	Tabular	No
Client Count	No	No	Graphical	No
Client Session	Yes	No	Tabular	No
Client Summary	Yes	Yes	Various	Yes
Client Traffic	No	No	Graphical	No
Client Traffic Stream Metrics	Yes	No	Tabular[1]	No
Posture Status Count	No	No	Graphical	No
Throughput	No	No	Tabular	No
Unique Clients	Yes	No	Tabular	No
CCX Client Statistics	No	No	Tabular	No
Configuration Audit	Yes	No	Tabular	No
PCI DSS Detailed	Yes	No	Tabular	No
PCI DSS Summary	No	No	Graphical	No
Client Location History	Yes	No	Tabular	No
Client Location Tracking	Yes	No	Tabular	No
Guest Location Tracking	Yes	No	Tabular	No
Location Notifications	Yes	No	Tabular	No
Rogue AP Location Tracking	Yes	No	Tabular	No
Rogue Client Location Tracking	Yes	No	Tabular	No
Tag Location History	Yes	No	Tabular	No
Tag Location Tracking	Yes	No	Tabular	No

Table 14-2 Report Customization (continued)

Report	Customizable?	Multiple SubReports?	Report Views	Data Field Sorting?
AP Image Pre-download				
AP Profile Status	Yes	No	Tabular	No
AP Summary				
Device Summary	Yes	No	Tabular	No
Busiest APs	Yes	No	Tabular	No
CPU Utilization	No	No	Graphical	No
Detailed Switch Inventory	Yes	Yes	Tabular	No
Identity Capability	No	No	Various	No
Inventory - Combined Inventory	Yes	Yes	Various[2]	Yes
Inventory - APs	Yes	Yes	Various	Yes
Inventory - Controllers	Yes	Yes	Various	Yes
Inventory - MSEs	Yes	Yes	Various	Yes
Up Time	Yes	No	Tabular	No
Utilization - Controllers	No	No	Graphical	No
Utilization - MSEs	No	No	Graphical	No
Utilization - Radios	No	No	Graphical	No
Guest Account Status	Yes	No	Tabular	No
Guest Association	Yes	No	Tabular	No
Guest Count	No	No	Tabular	No
Guest User Sessions	Yes	No	Tabular	No
NCS Guest Operations	Yes	No	Tabular	No
Mobile MAC Statistics	No	Yes	Tabular	No
Service URI Statistics	No	Yes	Tabular	No
Alternate Parent	Yes	No	Tabular	No
Link Stats - Link Stats	Yes	No	Tabular	No
Link Stats - Node Hops	No	No	Graphical	No
Nodes	Yes	No	Tabular	No
Packet Stats - Packet Stats	No	No	Graphical	No
Packet Stats - Packet Error Stats	No	No	Graphical	No
Packet Stats - Packet Queue Stats	No	No	Graphical	No
Stranded APs	No	No	Tabular	No

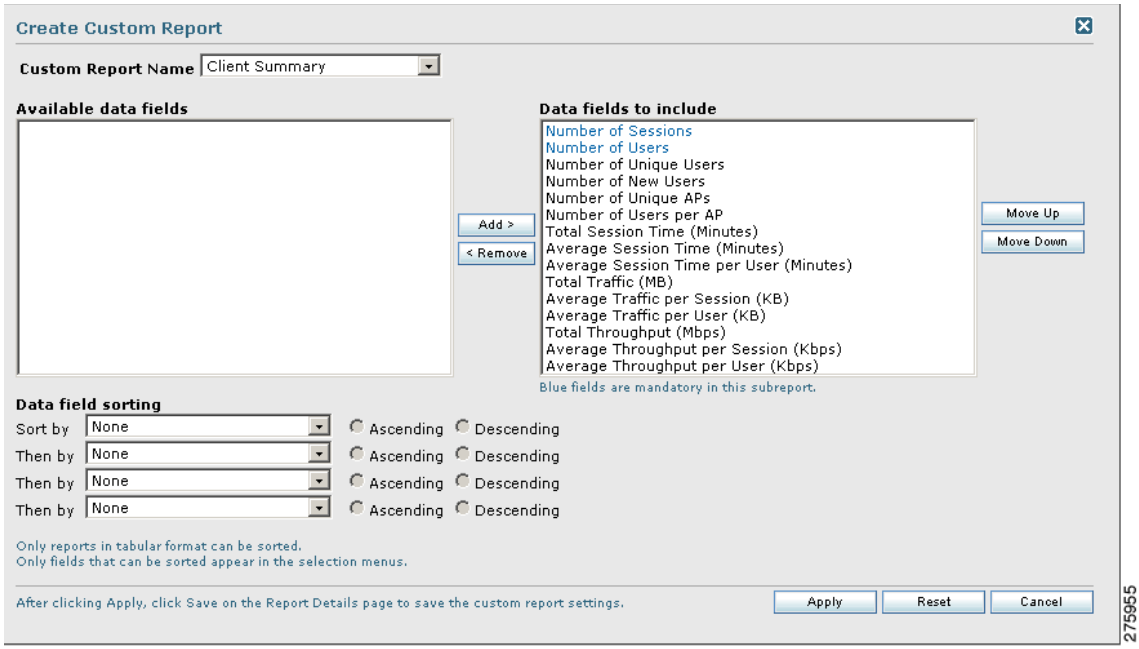
Table 14-2 Report Customization (continued)

Report	Customizable?	Multiple SubReports?	Report Views	Data Field Sorting?
Worst Node Hops - Worst Node Hop	Yes	Yes	Various	No
Worst Node Hops - Worst SNR Link	Yes	Yes	Various	No
802.11n Summary	No	Yes	Graphical	No
Executive Summary	No	Yes	Various	No
Preferred Calls	No	No	Graphical	No
802.11 Counters	Yes	No	Both	Yes
Coverage Holes	Yes	No	Tabular	No
Network Utilization	Yes	Yes	Both	Yes
Traffic Stream Metrics	Yes	Yes	Both	Yes
Tx Power and Channel	No	No	Graphical	No
VoIP Calls Graph	No	No	Graphical	No
VoIP Calls Table	No	No	Tabular	No
Voice Statistics	No	No	Graphical	No
Adaptive wIPS Alarm	Yes	No	Tabular	No
Adaptive wIPS Alarm Summary	Yes	No	Both	No
Adaptive wIPS Top 10 APs	Yes	No	Tabular	No
Adhoc Rogue Count Summary	Yes	No	Both	No
Adhoc Rogues	Yes	No	Tabular	No
New Rogue AP Count Summary	Yes	No	Both	No
New Rogue APs	No	No	Graphical	No
Rogue AP Count Summary	Yes	No	Both	No
Rogue APs	Yes	No	Tabular	No
Security Alarm Trending Summary	No	No	Graphical	No

1. Subreport Client Summary view is tabular only. The rest of the subreports such as Client Summary by Protocol have both report views and are customizable to show either tabular, graphical, or both.
2. Combined inventory report now contains APs/Controllers/MSEs/Autonomous APs/Switches. Reports that are by model or version have both views. These views are customizable with setting such as Count of Controllers by Model. Other reports, such as Controller Inventory, are tabular only.

Step 6 Click **Customize** to open a separate Create Custom Report page (see Figure 14-3).

Figure 14-3 Create Custom Report



a. From the Custom Report Name drop-down list, choose the report you intend to customize. The Available and Selected column heading selections might change depending on the report selected.

b. From the Report View drop-down list, specify if the report appears in tabular, graphical, or combined form (both). This option is not available on every report.

c. Use the **Add >** and **< Remove** buttons to move highlighted column headings between the two panes (Available data fields and Data fields to include).

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

d. Use the **Change Order** buttons (Move Up or Move Down) to determine the order of the columns in the results table. The higher the column heading appears in the Selected Columns list, the farther left it appears in the results table.

e. In the Data field Sorting section, indicate your sorting preference (Ascending or Descending). Determine how the report data is sorted.

- You can select four data fields for which you can specify sorting order. Use the Sort by and Then by drop-down lists to choose each data field for sorting.
- For each sorted data field, choose whether you want it sorted in Ascending or Descending order.

Note Only reports in table form (rather than graphs or combined) can be sorted. Only fields that can be sorted appear in the Data field sorting drop-down lists.

Note The Sortable fields displayed in the Create Custom Report page list all sortable fields irrespective of the data fields that are in the Data fields to include pane. The report is sorted based on the data field selected even if that column is not displayed in the report.

f. Click **Apply** to confirm the changes, **Reset** to return columns to the default, or **Cancel** to close this page with no changes made.

Note The changes made in the Create Custom Report page are not saved until you click **Save** on the Report Details page.

Step 7 When all report parameters have been set, choose one of the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Managing Current Reports

If a report has been saved for a specific report type, you can access the current reports from the Report Launch Pad.

Note You cannot change or update the generated reports together for all sub domains. You can open the generated reports individually through respective subdomains to change the reports. If all reports need to be updated, then delete all the reports created on subdomains and then regenerate the virtual domain reports using the add new report workflow with the changes.

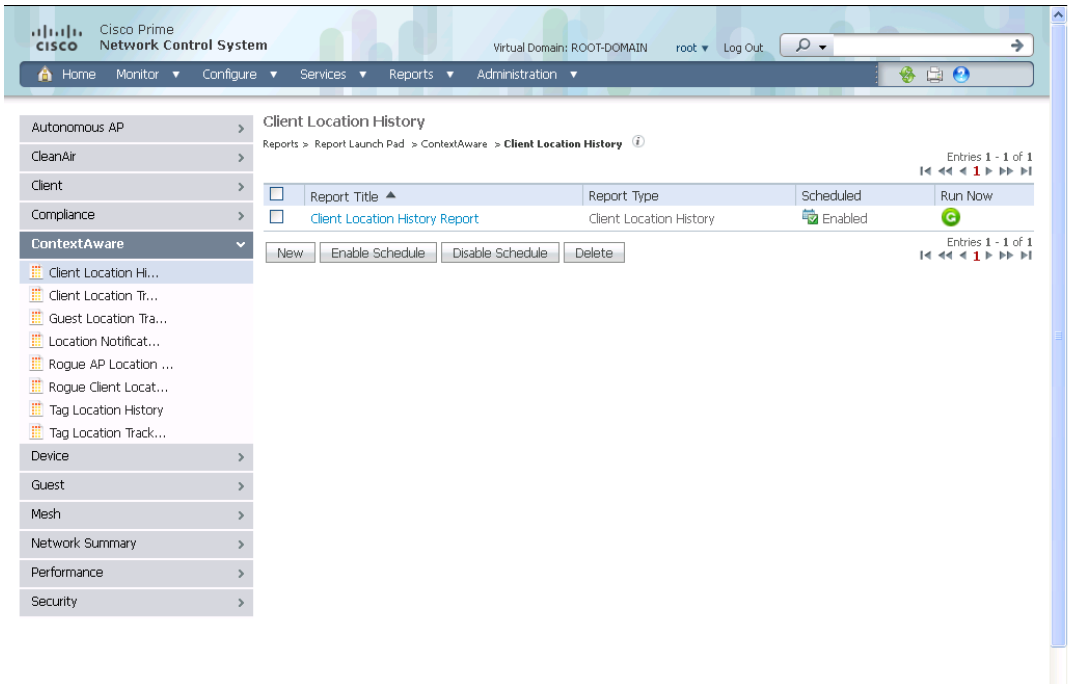
To access current or saved report templates from the Report Launch Pad or Saved Report Template, follow these steps:

Step 1 Choose **Reports > Report Launch Pad**.

Step 2 Choose the specific report from the left sidebar menu or from the main section of the Report Launch Pad. The page displays a list of current reports for this report type (see Figure 14-4).

Note To view a list of saved report templates, choose **Reports > Saved Report Templates**. See the "Managing Saved Report Templates" section on page 14-17 for more information.

Figure 14-4 Current Reports Page



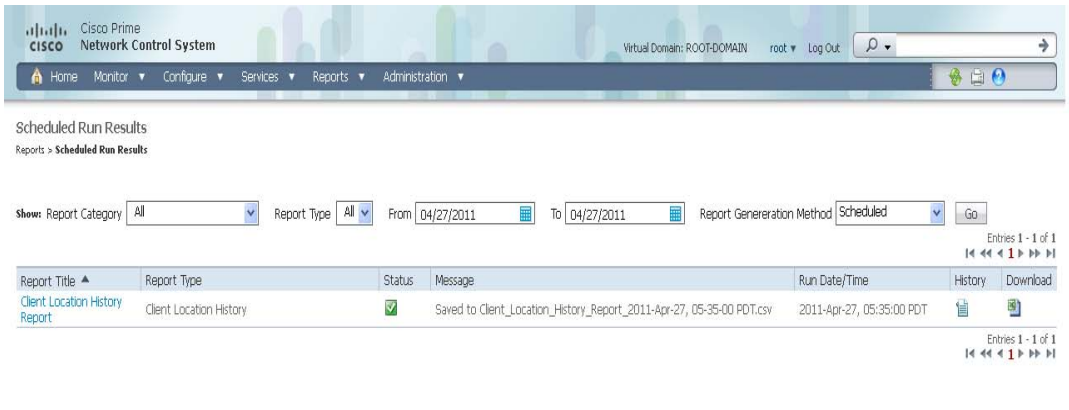
Managing Scheduled Run Results

To view all currently scheduled runs in the NCS, choose **Report > Scheduled Run Results** (see Figure 14-5).

Note The scheduled report tasks are not visible outside the Virtual Domain they run in. The results of the scheduled report tasks are visible from the Scheduled Run Results page of respective domains.

Note The list of scheduled runs can be sorted by report category, report type, and time frame.

Figure 14-5 Scheduled Run Results Page



The Scheduled Run Results page displays the following information:

- Report Title—Identifies the user-assigned report name.

Note Click the report title to view the details for this report.

- Report Type—Identifies the specific report type.
- Status—Indicates whether or not the report ran successfully.
- Message—Indicates whether or not this report was saved and the file name for this report (if saved).
- Run Date/Time—Indicates the date and time that the report is scheduled to run.
- History—Click the History icon to view all scheduled runs and their details for this report.
- Download—Click the Download icon to open or save a .csv/.pdf file of the report results.

For more information about scheduled run results, see the following:

- Sorting Scheduled Run Results, page 14-16
- Viewing or Editing Scheduled Run Details, page 14-17

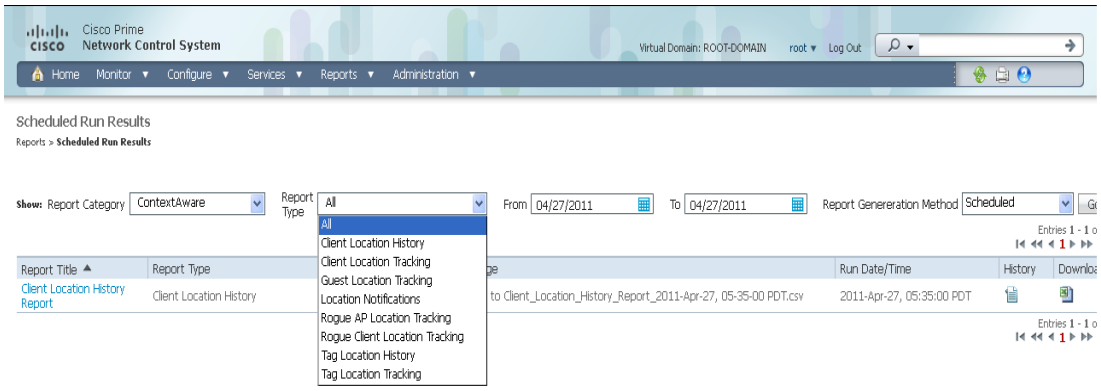
Sorting Scheduled Run Results

You can use the Show drop-down lists to sort the Scheduled Run Results by category, type, and time frame (see Figure 14-6):

- Report Category—Choose the appropriate report category from the drop-down list or choose **All**.
- Report Type—Choose the appropriate report type from the drop-down list or choose **All**. The report Type selections change depending on the selected report category.
- From/To—Type the report start (From) and end (To) dates in the text boxes or click the calendar icons to select the start and end dates.

Click **Go** to sort this list. Only reports that match your criteria appear.

Figure 14-6 Sorting Scheduled Run Results



Viewing or Editing Scheduled Run Details

To view or edit a saved report template, follow these steps:

Step 1 Choose **Report > Scheduled Run Results**.

Step 2 Click the Report Title link for the appropriate report to open the Report Details page.

Step 3 From this page, you can view or edit the details for the scheduled run.

Step 4 When all scheduled run parameters have been edited (if necessary), select from the following:

- Save—Click to save this schedule run without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this scheduled run and to immediately run the report.
- Cancel—Click to return to the previous page without running nor saving this report.
- Delete—Click to delete the current saved report template.

Managing Saved Report Templates

In the Saved Report Templates page, you can create and manage saved report templates (see Figure 14-7). To open this page in the NCS, choose **Reports > Saved Report Templates**.

Note The list of saved report templates can be sorted by report category, report type, and scheduled status (enabled, disabled, or expired).

Figure 14-7 Saved Report Templates Page

The Saved Report Templates page displays the following information:

- Report Title—Identifies the user-assigned report name.

Note Click the report title to view the details for this report.

- Report Type—Identifies the specific report type.
- Scheduled—Indicates whether this report is enabled or disabled.
- Run—Click the **Run** icon to immediately run the current report.

This section contains the following topics:

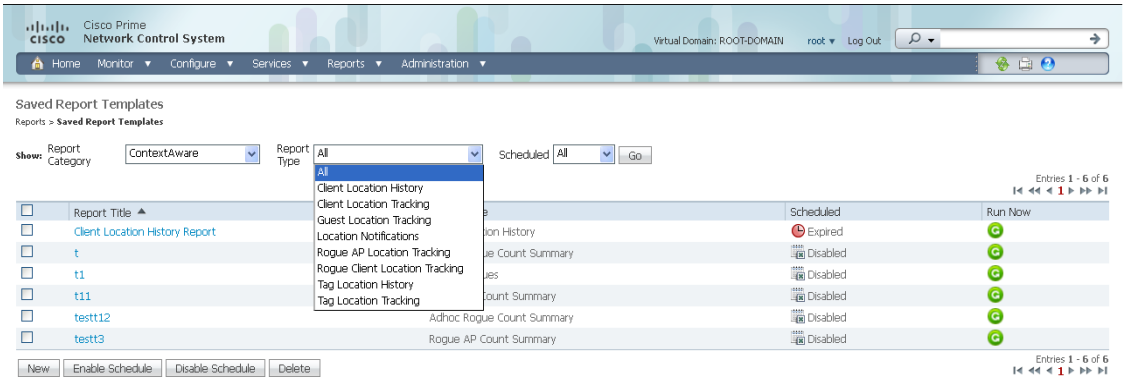
- Filtering Saved Report Templates, page 14-18
- Viewing or Editing Saved Report Template Details, page 14-19
- Running a Saved Report Template, page 14-19

Filtering Saved Report Templates

You can use the Show drop-down lists to filter the Saved Report Templates list by category, type, and scheduled status (see Figure 14-8).

- Report Category—Choose the appropriate report category from the drop-down list or choose **All**.
- Report Type—Choose the appropriate report type from the drop-down list or choose **All**. The Report Type selections change depending on the selected report category.
- Scheduled—Choose **All**, **Enabled**, **Disabled**, or **Expired** to filter the Saved Report Templates list by scheduled status.

Figure 14-8 Filtering Saved Report Templates



Click **Go** to filter this list. Only reports that match your criteria appear.

•

Viewing or Editing Saved Report Template Details

To view or edit a saved report template, follow these steps:

Step 1 Choose **Report > Saved Report Templates**.

Step 2 Click the Report Title link for the appropriate report to open the Report Details page.

Step 3 From this page, you can view or edit the details for the saved report template.

Step 4 When all report parameters have been edited, choose one of the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Cancel—Click to return to the previous page without running nor saving this report.
- Delete—Click to delete the current saved report template.

Running a Saved Report Template

In the Reports > Saved Report Templates page, click **Run** for the appropriate report. This section describes the reports specific to the NCS and contains the following topics:

- Autonomous AP Reports, page 14-22
  - Autonomous AP Memory and CPU Utilization, page 14-22
  - Autonomous AP Summary, page 14-24
  - Autonomous AP Tx Power and Channel, page 14-26
  - Autonomous AP Uptime, page 14-28
  - Autonomous AP Utilization, page 14-30

Autonomous AP Reports

This section lists and describes the various Autonomous AP reports that you can generate in the NCS. Click **New** next to the Autonomous AP report category to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

This section describes the Autonomous AP reports and contains the following topics:

Autonomous AP Memory and CPU Utilization

This report displays the memory and CPU utilization trends of Autonomous access points based on the filtering criteria specified during report generation. It could help in identifying unexpected behavior or issues with network performance.

This section contains the following topics:

Configuring an Autonomous AP Memory and CPU Utilization Report

This section describes how to configure an Autonomous AP Memory and CPU Utilization report.

Settings

The following settings can be configured for a Autonomous AP Memory and CPU Utilization report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - Autonomous AP IP Address—Choose from the Report Criteria list or click **Edit** to choose specific access points.
  - Autonomous AP Host Name—Choose from the Report Criteria list or click **Edit** to choose specific access points.
- Reporting Period—You can configure the reporting period in two ways:
  - Last—Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note Leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

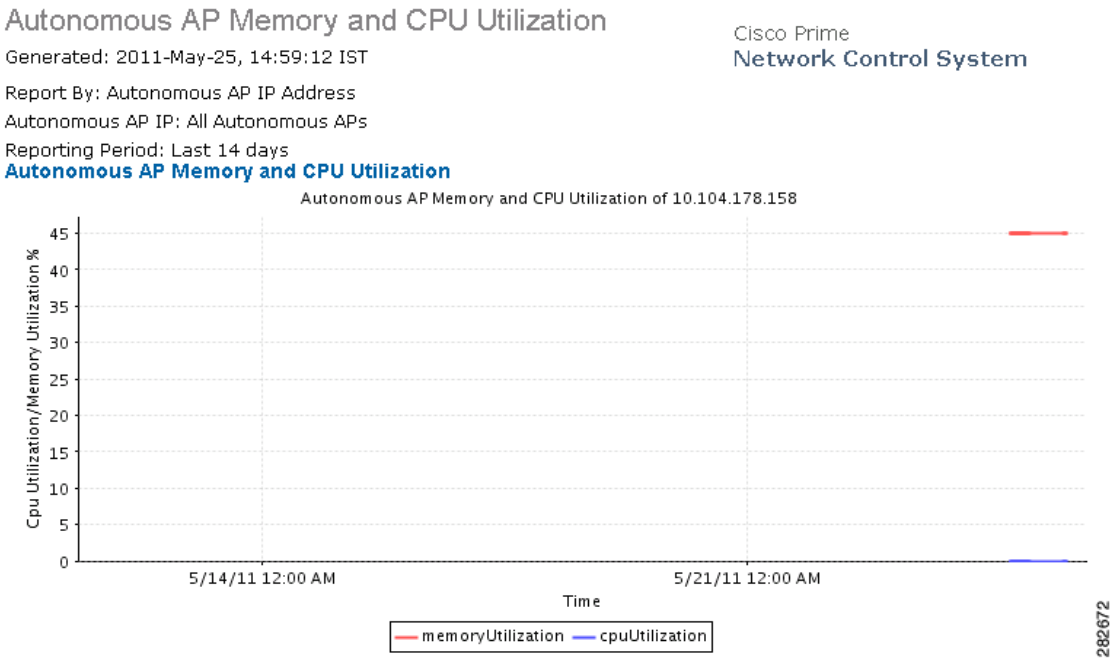
Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Autonomous AP Memory and CPU Utilization Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Figure 14-9 shows the potential results for an Autonomous AP Memory and CPU Utilization report, depending on how the report is customized.

Figure 14-9 Autonomous AP Memory and CPU Utilization Report



Autonomous AP Summary

This report displays the Autonomous AP summary.

This section contains the following topics:

- Configuring the Autonomous AP Summary Report, page 14-24
- Autonomous AP Summary Report Results, page 14-25

Configuring the Autonomous AP Summary Report

This section describes how to configure an Autonomous AP Summary report.

Settings

The following settings can be configured for a Autonomous AP Summary report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - Autonomous AP IP Address—Choose from the Report Criteria list or click **Edit** to choose specific access points.
  - Autonomous AP Host Name—Choose from the Report Criteria list or click **Edit** to choose specific access points.
  - Floor Area—Choose **All Campuses > All Buildings > All Floors** or click **Edit** to choose specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Areas** or click **Edit** to choose specific locations.

Note Leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Creating a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Autonomous AP Summary Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for an Autonomous AP Summary report, depending on how the report is customized:

- AP Name
- Ethernet MAC Address
- AP IP Address
- Model
- Map Location

Autonomous AP Tx Power and Channel

This report displays the channel plan assignment and transmits power level trends of devices based on the filtering criteria used when the report was generated. It can help identify unexpected behavior or issues with network performance.

This section contains the following topics:

- Configuring an Autonomous AP Tx Power and Channel Report, page 14-26
- Autonomous AP Tx Power and Channel Report Results, page 14-27

Configuring an Autonomous AP Tx Power and Channel Report

This section describes how to configure an Autonomous AP Tx Power and Channel report.

Settings

The following settings can be configured for an Autonomous AP Tx Power and Channel report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - Autonomous AP IP Address—Choose from the Report Criteria list or click **Edit** to choose specific access points.
  - Autonomous AP Host Name—Choose from the Report Criteria list or click **Edit** to choose specific access points.
  - Autonomous AP By Floor Area—Choose **All Campuses > All Buildings > All Floors** or click **Edit** to choose specific locations.
  - Autonomous AP By Outdoor Area—Choose **All Campuses > All Outdoor Areas** or click **Edit** to choose specific locations.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last—Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

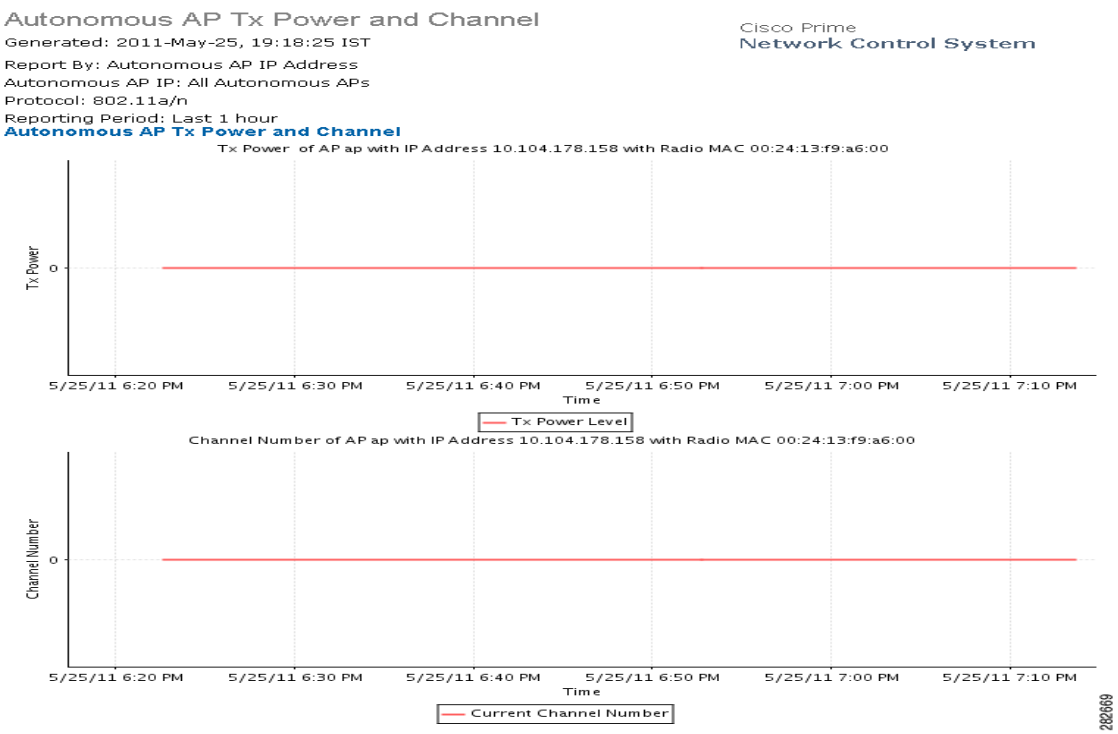
Autonomous AP Tx Power and Channel Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following information is displayed for a Tx Power and Channel report (see Figure 14-10):

- Transmit power level for each access point during the specified period of time.
- Channel number for each access point during the specified period of time.

Figure 14-10 Autonomous AP Tx Power and Channel Report



Autonomous AP Uptime

This report displays the Autonomous AP uptime.

This section contains the following topics:

- Configuring Autonomous AP Uptime Report
- Autonomous AP Uptime Report Results

Configuring Autonomous AP Uptime Report

This section describes how to configure an Autonomous AP Uptime report.

Settings

The following settings can be configured for an Autonomous AP Uptime report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - Autonomous AP IP Address—Choose from the Report Criteria list or click **Edit** to choose specific access points.
  - Autonomous AP Host Name—Choose from the Report Criteria list or click **Edit** to choose specific access points.

  - Autonomous AP By Floor Area—Choose **All Campuses > All Buildings > All Floors** or click **Edit** to choose specific locations.
  - Autonomous AP By Outdoor Area—Choose **All Campuses > All Outdoor Areas** or click **Edit** to choose specific locations.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Autonomous AP Uptime Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for an Autonomous AP Uptime report, depending on how the report is customized:

- AP Name
- IP Address
- Map Location

- AP Up Time

Autonomous AP Utilization

This report displays the utilization trends of Autonomous AP radios based on the filtering criteria used when the report was generated. It can help identify current network performance and capacity planning for future scalability needs.

This section contains the following topics:

- Configuring an Autonomous AP Utilization Report, page 14-30
- Autonomous AP Utilization Report Results, page 14-31

Configuring an Autonomous AP Utilization Report

This section describes how to configure an Autonomous AP Utilization report.

Settings

The following settings can be configured for a Autonomous AP Utilization report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - Autonomous AP IP Address—Choose from the list or click **Edit** to choose specific access points.
  - Autonomous AP Host Name—Choose **System Campus > All Access Points** or click **Edit** to choose specific access points.
  - Autonomous AP Floor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click **Edit** to choose specific locations or access points.
  - Autonomous AP Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click **Edit** to choose specific locations or access points.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last—Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note Leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

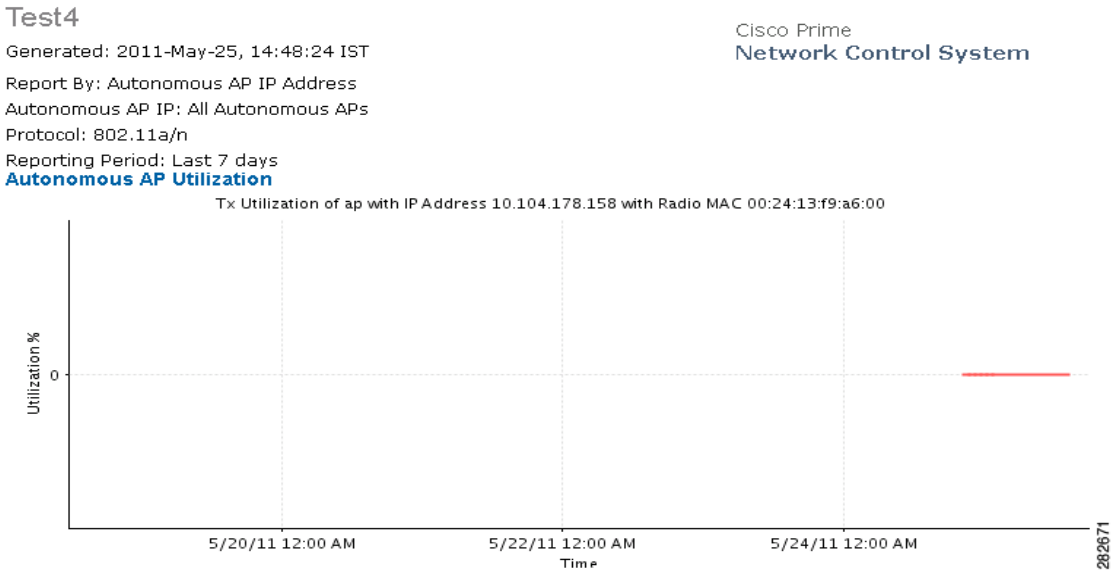
Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Autonomous AP Utilization Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Figure 14-11 shows the potential results for an Autonomous AP Utilization report, depending on how the report is customized.

Figure 14-11 Autonomous AP Utilization Report



Busiest Autonomous APs

This report displays the Autonomous APs with the highest total usage (the sum of transmitting, receiving, and channel usage) on your wireless network.

Configuring a Busiest Autonomous APs Report

This section describes how to configure a Busiest Autonomous APs report.

Settings

The following settings can be configured for a Busiest Autonomous APs report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - Autonomous AP IP Address—Choose from the list or click **Edit** to choose specific access points.
  - Autonomous AP Host Name—Choose **System Campus > All Access Points** or click **Edit** to choose specific access points.
  - Autonomous AP Floor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click **Edit** to choose specific locations or access points.
  - Autonomous AP Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** or click **Edit** to choose specific locations or access points.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last—Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Busiest Autonomous APs Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Busiest Autonomous APs report, depending on how the report is customized:

- IP Address
- AP Name
- Rx Utilization (%)
- Tx Utilization (%)
- Map Location
- Client Count

CleanAir Reports

Click **New** for CleanAir report type to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

This section describes the CleanAir reports and contains the following topics:

Air Quality vs Time

This report displays the air quality index distributions over a period of time for access points on your wireless networks.

Click **Air Quality vs Time** from the Report Launch Pad to open the Air Quality vs Time page. In this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Air Quality vs Time page. See the "Configuring an Air Quality vs Time Report" section on page 14-34 and the "Air Quality vs Time Report Results" section on page 14-35 for more information.

Configuring an Air Quality vs Time Report

This section describes how to configure an Air Quality vs Time report.

Settings

The following settings can be configured for an Air Quality vs Time report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - AP By Controller—Choose **All Controllers > All Access Points**, or click **Edit** to choose specific access points.
  - AP By Floor Area—Choose **System Campus > All Access Points**, or click **Edit** to choose specific access points.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points**, or click **Edit** to choose specific locations or access points.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last—Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Air Quality vs Time Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are the potential results for an Air Quality vs Time report, depending on how the report is customized:

- AP Name
- MAC Address
- Radio Type
- Time
- AQ Minimum Index
- AQ Average Index

Security Risk Interferers

This report displays the security risk interferers on your wireless network.

Click **Security Risk Interferers** from the Report Launch Pad to open the Security Risks Interferers page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Security Risk Interferers page. See the "Configuring a Security Risk Interferers Report" section on page 14-36 and the "Security Risks Interferers Report Results" section on page 14-37 for more information.

Configuring a Security Risk Interferers Report

This section describes how to configure a Security Risk Interferers report.

Settings

The following settings can be configured for a Security Risks Interferers report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - AP By Controller—Choose **All Campuses > All Buildings > All Floors > All Access Points**, or click **Edit** to choose specific access points.
  - AP By Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points**, or click **Edit** to choose specific access points.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points**, or click **Edit** to choose specific locations or access devices.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last—Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Note The information in this report is available only if you set a security alarm on the interferer.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.

- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Security Risks Interferers Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Security Risks Interferers report, depending on how the report is customized:

- Interferer Type
- Affected Channels
- Discovered
- Last Updated
- Detected AP Name
- Affected Band

Worst Air Quality APs

This report displays the access points with the lowest air quality index.

Click **Worst Air Quality APs** from the Report Launch Pad to open the Worst Air Quality APs page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Worst Air Quality APs page. See the "Configuring a Worst Air Quality APs Report" section on page 14-37 and the "Worst Air Quality APs Report Results" section on page 14-39 for more information.

Configuring a Worst Air Quality APs Report

This section describes how to configure a Worst Air Quality APs report.

Settings

The following settings can be configured for a Worst Air Quality APs report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By

  - AP By Controller—Choose **All Campuses > All Buildings > All Floors > All Access Points**, or click **Edit** to choose specific access points.
  - AP By Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points**, or click **Edit** to choose specific access points.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points**, or click Edit to choose specific locations or access devices.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last—Select the first radio button to generate reports for a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

- Air Quality Index Threshold—Select this check box if you want to set an air quality index threshold. The text box next to the check box appears enabled when you select the Air Quality Index Threshold check box. Enter a threshold between 1 and 100. Default threshold value is 70.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Worst Air Quality APs Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Worst Air Quality APs report, depending on how the report is customized:

- AP Name
- Radio Type
- Worst Air Quality Value
- Channel Number
- Most Recent Reported Time
- Interferer Count

Worst Interferers

This report displays the worst interferers on your wireless network.

Click **Worst Interferers** from the Report Launch Pad to open the Worst Air Quality APs page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Worst Interferers page.

Configuring a Worst Interferers Report

This section describes how to configure a Worst Interferers report.

Settings

The following settings can be configured for a Worst Interferers report:

- Report Title—If you plan to use this as a saved report template, type an appropriate name.
- Report By
  - Cluster Center AP
  - Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the report criteria area, or click **Edit** to choose specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Area** from the report criteria area, or click **Edit** to choose specific locations.
- Protocol—Select the radio type by selecting the check box specific to a radio frequency.
- Reporting Period—You can configure the reporting period in two ways:
  - Last—Select the first radio button to generate reports for a period of time from the drop-down list.

  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Create a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Worst Interferers Report Results

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Worst Interferers report, depending on how the report is customized:

- Device Type
- Severity
- Worst Severity Time
- Duty Cycle (%)

- Affected Channels
- Cluster Center APs
- Map Location
- Discovered

Note Severity value N/A means that the severity value for this device is not available. A value of 1 means that the severity is minimal and a value of 100 means very severe.

Note Interferers with an unknown location are not listed if the Report By criteria is Floor Area or Outdoor Area.

Client Reports

The report structure has changed in Release 6.0 or later:

- The Client Association and Detailed Client reports are replaced by the Client Session report.
- Any saved Detailed Client reports are migrated to the Client Session report.
- Client Association data from 5.1 or earlier is not migrated.

  Note After migration to 6.0 or later releases, you cannot see previous Client Association information that was presented in the Client Association report.

- The Client Count report that was under 802.11 Scaling in Release 5.2 is now consolidated into one Client Count report.

Note When you create a virtual domain in reports, the statistcs collection for the virtual domain starts after its creation. Therefore, you do not get the hourly statistics for the previous hours (prior to the creation of the virtual domain) as you get the statistcs for the ROOT-DOMAIN.

This section describes the types of client reports available and contains the following topics:

Busiest Clients

This report displays the busiest and least busy clients on the wireless network by throughput, utilization, and other statistics. You can sort this report by location, by band, or by other parameters.

Note Busiest Clients reports do *not* include autonomous clients.

Click Busiest Clients from the Report Launch Pad to open the Busiest Clients Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

Configuring a Busiest Clients Report

This section describes how to configure a Busiest Clients report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - Controller—Choose **All Controllers** from the Report Criteria page, or click **Edit** to choose specific devices.
  - Floor Area—Choose **All Campuses > All Buildings > All Floors** from the Report Criteria page, or click **Edit** to choose specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Areas** from the Report Criteria page, or click **Edit** to choose specific locations.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - SSID—Choose **All SSIDs** from the Report Criteria page or click **Edit** to choose a specific or multiple SSIDs.
  - AP by RAP Mesh Role—Choose **All RAP APs** from the Report Criteria page, or click **Edit** to choose a specific RAP access point.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Connection Protocol—Choose **All Clients**, **Wired Clients**, or a specific radio type from the drop-down list.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Click **From** and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the clients last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Creating a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Available information for the Busiest Client report results contains the following:

- Client MAC Address—The MAC address of the client.
- Client IP Address—The IP address of the client.
- Username
- Protocol—802.11a, 802.11b, 802.11g, 802.11n_5 GHz, or 802.11n_2.4 GHz
- Throughput (Mbps)—The average throughput (in Mbps) for the client.
- Utilization (%)—The average percentage of use for this client.
- On Controller—The controller on which the client is located.
- Bytes Sent—The number of bytes sent.
- Bytes Received—The number of bytes received.
- Packets Sent—The number of packets sent.
- Packets Received—The number of packets received.

Busiest Clients Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following potential results occur, depending on how the report is customized (see Figure 14-12):

- Client MAC address
- IP address—The IP address of the client. This field displays IPv6 address for IPv6 clients and IPv4 address for IPv4 and dual stack clients.
- Username
- Protocol—802.11a/n or 802.11b/g/n
- Throughput—Either Mbps or kbps

Note If throughput is less than 0.1 kbps, you see <0.1 kbps.

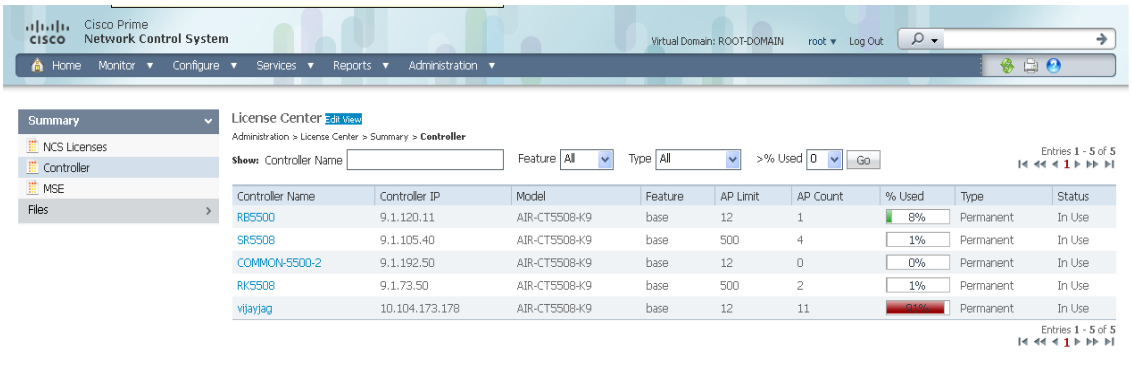
- Utilization (%)
- Global Unique—The aggregate global unicast address of an IPv6 address. This field is populated only if a client is assigned a Global Unique IPv6 address.
- Local Unique—The local unicast address of an IPv6 address. This field is populated only if a client is assigned a Local Unique IPv6 address.
- Link Local—The link local unicast address of an IPv6 address. This field is populated only if a client is assigned a Link Local IPv6 address.
- On Device—The device on which the client is located.
- Bytes sent (MB)—The number of bytes sent in MB.
- Bytes received (MB)—The number of bytes received in MB.

Note If the value is greater than 1,000,000,000, a G is appended at the end of the value (such as 3.45 G). If the value is greater than 1,000,000 but less than 1,000,000,000, an M is appended at the end of the value (such as 456.8 M).

- Packets Sent
- Packets Received

Note If the value is greater than 1,000,000,000, a G is appended at the end of the value (such as 3.45 G). If the value is greater than 1,000,000 but less than 1,000,000,000, an M is appended at the end of the value (such as 456.8 M).

Figure 14-12 Busiest Client Report Results



Client Count

This trending report displays the total number of active clients on your wireless network.

The Client Count report displays data on the numbers of clients that connected to the network through a specific device, in a specific geographical area, or through a specific or multiple SSIDs.

Note Client Count reports include clients connected to autonomous Cisco IOS access points.

Note You cannot upgrade the Client Count report to the NCS Release 1.0 and later.

Note When you run the client count report for two different sub virtual domains under the root domain, the data reported might be the same even if the controllers assigned to the two virtual domains are different. This is because the report returns data for all the controllers in the system. If you want to get a separate report for a virtual domain, run the report as a particular virtual domain user other than a root domain user.

Configuring a Client Count Report

This section describes how to configure a Client Count report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - All—Choose All if you want a count of all clients in the network.
  - Controller IP Address—Choose **Controller IP Address** if you want a count of the clients that are associated to all or specific controller in the network.
  - Controller Host Name—Choose **Controller Host Name** if you want a count of the clients that are associated to all or specific controller in the network.
  - Autonomous AP IP Address—Choose **Autonomous AP IP Address** if you want a count of all autonomous APs in the network.
  - Autonomous AP Host Name—Choose **Autonomous AP Host Name** if you want a count of all autonomous APs in the network.
  - Switch IP Address—Choose **Switch IP Address** if you want a count of all switches in the network.
  - Switch Host Name—Choose **Switch Host Name** if you want a count of all switches in the network.
  - Floor Area—Choose **Floor Area** if you want a count of all the clients in a floor in the network.
  - Outdoor Area—Choose **Floor Area** if you want a count of all the clients in an outdoor area in the network.
  - AP by Floor Area—Choose **AP by Floor Area** if you want a count of all the access points in a floor in the network.
  - AP by Outdoor Area—Choose **AP by Outdoor Area** if you want a count of all the access points in an outdoor area in the network.
  - SSID—Choose **SSID** if you want a count of all the clients in a network-based on SSID.

  - AP by RAP Mesh Role—Choose **AP by RAP Mesh Role** if you want a count of all the RAP Mesh access points in the network.

- Report Criteria—Either choose the corresponding option from the drop-down list or click **Edit** to choose specific devices.The options vary based on the Report By option you had chosen.

Note In the Report Criteria page, click **Select** to confirm your sort criteria or **Close** to return to the previous page.

- Connection Protocol—Choose **All Clients** or a specific radio type from the drop-down list.

Note Wired clients and clients associated to Cisco IOS access points are not included as part of this report.

- SSID—By default this option is All SSIDs.

Note This SSID also works as a second level filter if the report criteria is selected as not ALL. For example, if you choose Report By as Controller IP, Report Criteria as choose any controller, then the SSID filter becomes active and you can choose any SSID to run the report.

- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report

The Customize button is available for this report but it does not customize the report as intended.

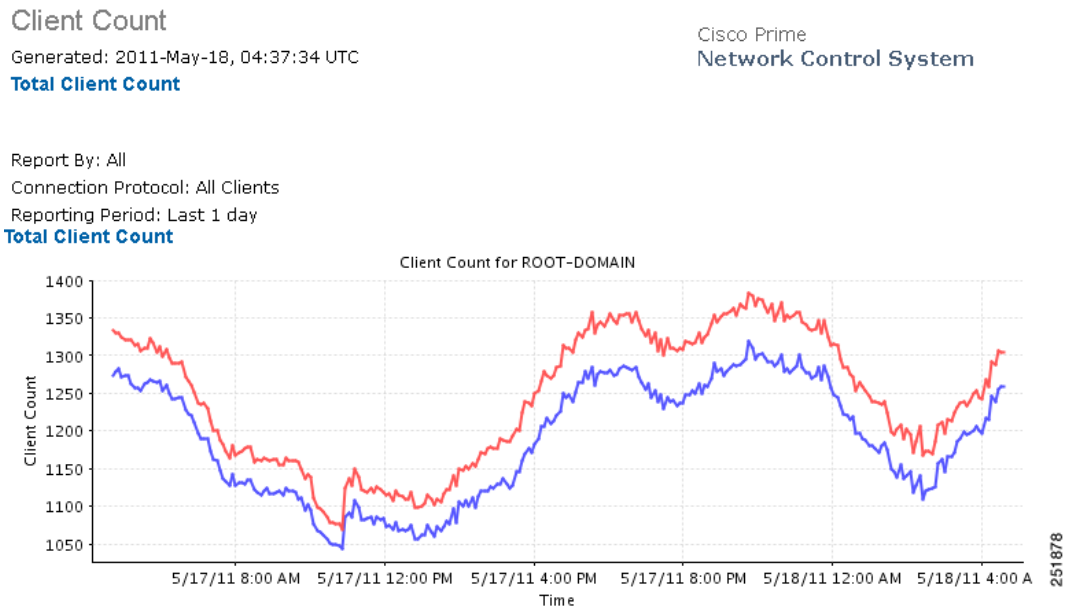
Client Count Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Client Count report, depending on how the report is customized (see Figure 14-13):

- Client IP address
- AP Name
- Key
- SSID
- Date and time the count was taken
- Associated client count
- Authenticated client count

Figure 14-13 Client Count Report Results



Client Sessions

This report provides client sessions for the given period of time. It displays the history of client sessions, statistics, and the duration at which clients are connected to an access point at any given period of time.

Click **Client Sessions** from the Report Launch Pad to open the Client Sessions Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

Configuring a Client Sessions Report

This section describes how to configure a Client Sessions report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - Controller—Choose **All Controllers** from the Report Criteria page, or click **Edit** to choose specific devices.
  - Floor Area—Choose **All Campuses > All Buildings > All Floors** from the Report Criteria page, or click **Edit** to choose specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Areas** from the Report Criteria page, or click **Edit** to choose specific locations.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - SSID—Choose **All SSIDs** from the Report Criteria page, or click **Edit** to choose a specific or multiple SSIDs.
  - AP by RAP Mesh Role—Choose **All RAP APs** from the Report Criteria page, or click **Edit** to choose a specific RAP access point.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

  - VLAN
  - Client MAC Address
  - Client Username
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Available information for Client Sessions report results contain the following:

- Host Name—The DNS hostname of the device the client is on. The NCS performs a DNS lookup to resolve the hostname from the IP address of the client. The IP address to hostname mapping must be defined in a DNS server. By default, the hostname lookup is disabled. Use **Administration > Settings > Clients** to enable hostname lookup.
- Client Type
- Global Unique—The aggregate global unicast address of an IPv6 address. This field is populated only if a client is assigned a global unique IPv6 address.
- Local Unique—The local unicast address of an IPv6 address. This field is populated only if a client is assigned a local unique IPv6 address.
- Link Local—The link local unicast address of an IPv6 address. This field is populated only if a client is assigned a link local IPv6 address.
- Speed
- CCX—The Cisco Client Extension version number.
- AP MAC Address
- IP address—The IP address of the client. This field displays IPv6 address for IPv6 clients and IPv4 address for IPv4 and dual stack clients.
- AP Radio—The radio type of the access point.
- Device IP Address—The IP address of the device to which this client is associated.
- Port—The port number for the device to which this client is associated.
- Anchor Controller—The IP address of the anchor or foreign controller for the mobility client.
- Association ID—The association ID used for the client session.
- Disassociation Time—The date and time this client disassociated.
- Authentication—The authentication method for this client.
- Encryption Cypher—Encryption cypher used in this client session.
- EAP Type—EAP type used in this client session.
- Authentication Algorithm—Authentication algorithm used in this client session.
- Web Security—Web security used in this client session.
- Bytes Sent (MB)—The approximate number of bytes transmitted during the session.
- Bytes Received (MB)—The approximate number of bytes received during the session.
- Packet Sent
- Packets Received
- SNR (dBm)—Signal-to-noise ratio for this client session indicated in dBm.
- RSSI—The Received Signal Strength Indicator in dBm.

- Status—Associated or disassociated.
- Reason—Reason for disassociation.
- E2E—Version number or *Not Supported*.
- Data Retries
- RTS Retries

Client Sessions Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

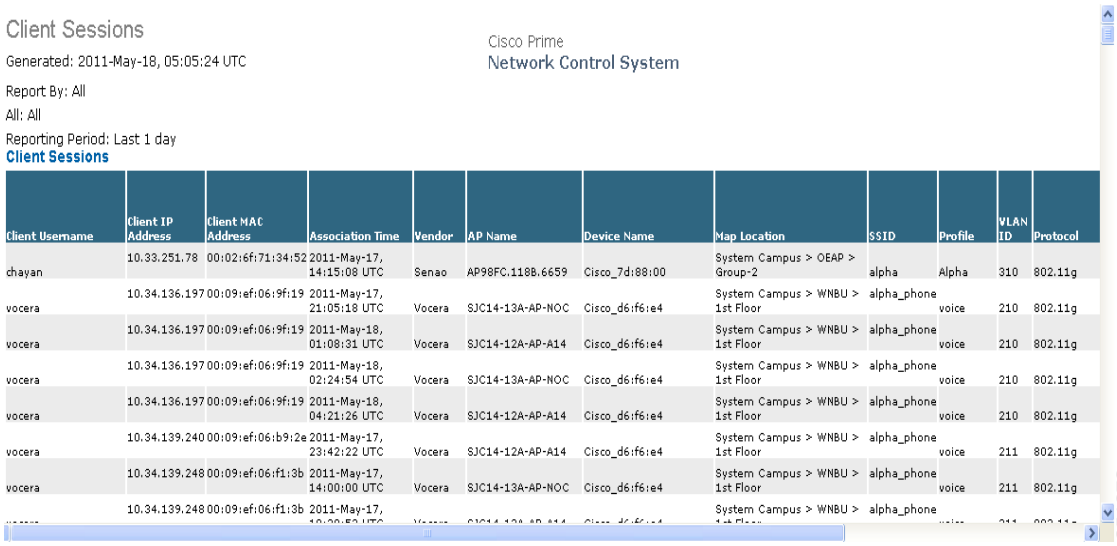
The following are potential results for a Client Sessions report, depending on how the report is customized (see Figure 14-14):

- Client username, IP address, and MAC address (mandatory columns)
- Association time (mandatory column)
- Vendor
- Access point name—The access point name to which this client is assigned.
- Controller names
- Map Location—The building, floor area, or outdoor area (as applicable) where the client is located.
- SSID—The SSID to which this client is associated.
- Profile—The name of the profile to which this client is associated.
- VLAN ID—The VLAN Identifier. The range is 1 to 4096.
- Protocol—802.11a, 802.11b, 802.11g, 802.11n_5GHz, or 802.11b_2.4GHz.
- Session Duration
- Policy Type—The type of security policy for this client session.
- Average Session Throughput (kbps)
- Host Name—The DNS hostname of the machine on which this client is located.

  The NCS performs a DNS lookup to resolve the hostname from the client IP address. The IP address to hostname mapping must be defined in a DNS server. By default, the hostname lookup is disabled. Use **Administration > Settings > Clients** to enable hostname lookup.
- Client Type
- Global Unique—The aggregate global unicast address of an IPv6 address. This field is populated only if a client is assigned a global unique IPv6 address.
- Local Unique—The local unicast address of an IPv6 address. This field is populated only if a client is assigned a local unique IPv6 address.
- Link Local—The link local unicast address of an IPv6 address. This field is populated only if a client is assigned a link local IPv6 address.
- CCX—The Cisco Client Extension version number.
- AP MAC address
- IP address

- AP Radio—The radio type of the access point.
- Device IP address
- Device Port—The port number for the device to which this client is associated.
- Anchor Controller—The IP address of the anchor or foreign controller for the mobility client, if applicable.
- Association ID—Association ID used in this client session.
- Disassociation Time—The date and time this client disassociated.
- Authentication—The authentication method for this client.
- Encryption Cypher—Encryption cypher used in this client session.
- EAP Type—EAP type used in this client session.
- Authentication Algorithm—Authentication algorithm used in this client session.
- Web Security—Web security used in this client session.
- Tx and Rx (bytes)—The approximate number of bytes transmitted or received during the client session.
- Packets sent and received
- SNR—Signal-to-noise ratio for this client session.
- RSSI—The Received Signal Strength Indicator in dBm.
- Status—Associated or disassociated.
- Reason—Reason for disassociation.
- E2E—Version number or *Not Supported*.

Figure 14-14 Client Sessions Report Results



Client Sessions

Generated: 2011-May-18, 05:05:24 UTC

Report By: All

All: All

Reporting Period: Last 1 day

Cisco Prime
Network Control System

Client Sessions

Client Username	Client IP Address	Client MAC Address	Association Time	Vendor	AP Name	Device Name	Map Location	SSID	Profile	VLAN ID	Protocol
chayan	10.33.251.78	00:02:6f:71:34:52	2011-May-17, 14:15:08 UTC	Senao	AP98FC.118B.6659	Cisco_7d:88:00	System Campus > OEAP > Group-2	alpha	Alpha	310	802.11g
vocera	10.34.136.197	00:09:ef:06:9f:19	2011-May-17, 21:05:18 UTC	Vocera	SJC14-13A-AP-NOC	Cisco_d6:f6:e4	System Campus > WNBU > 1st Floor	alpha_phone	voice	210	802.11g
vocera	10.34.136.197	00:09:ef:06:9f:19	2011-May-18, 01:08:31 UTC	Vocera	SJC14-12A-AP-A14	Cisco_d6:f6:e4	System Campus > WNBU > 1st Floor	alpha_phone	voice	210	802.11g
vocera	10.34.136.197	00:09:ef:06:9f:19	2011-May-18, 02:24:54 UTC	Vocera	SJC14-13A-AP-NOC	Cisco_d6:f6:e4	System Campus > WNBU > 1st Floor	alpha_phone	voice	210	802.11g
vocera	10.34.136.197	00:09:ef:06:9f:19	2011-May-18, 04:21:26 UTC	Vocera	SJC14-12A-AP-A14	Cisco_d6:f6:e4	System Campus > WNBU > 1st Floor	alpha_phone	voice	210	802.11g
vocera	10.34.139.240	00:09:ef:06:b9:2e	2011-May-17, 23:42:22 UTC	Vocera	SJC14-12A-AP-A14	Cisco_d6:f6:e4	System Campus > WNBU > 1st Floor	alpha_phone	voice	211	802.11g
vocera	10.34.139.248	00:09:ef:06:f1:3b	2011-May-17, 14:00:00 UTC	Vocera	SJC14-13A-AP-NOC	Cisco_d6:f6:e4	System Campus > WNBU > 1st Floor	alpha_phone	voice	211	802.11g
[illegible]	10.34.139.248	00:09:ef:06:f1:3b	2011-May-17, [illegible]	Vocera	[illegible]	[illegible]	System Campus > WNBU > [illegible]	alpha_phone	[illegible]	[illegible]	[illegible]

251879

Client Summary

The Client Summary is a detailed report that displays various client statistics.

Click Client Summary from the Report Launch Pad to open the Client Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

Note You cannot upgrade the Client Summary reports to the NCS Release 1.0 and later.

Configuring a Client Summary Report

This section describes how to configure a Client Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Note The data for the Client Summary report is computed at backend. The report uses the computed data only. The data is computed every hour for one day and every night for a year. Therefore, you would only be able to create hourly-based Client Summary reports for the last 24 hours.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Note A Client Summary report contains summary results sorted by protocol, SSID, VLAN, and vendor. To customize report results for a particular section, choose the applicable section from the Customizable Report drop-down list.

The Client Summary report contains four sub reports. Each of them can be independently customized. The following is default information available from a Client Summary report depending on the customizable report selected:

- Number of Sessions
- Number of Total Users
- Number of Unique Users
- Number of New Users
- Number of Unique APs
- Number of Users per AP
- Total Traffic (MB)
- Average Traffic per Session (KB) and per user (in KB)
- Total Throughput (Mbps)
- Average Throughput per Session and per user (Mbps)

  Note When the NCS does not receive client traps, it relies on client status polling to discover client associations (The task runs every 5 minutes by default.). However, the NCS cannot accurately determine when the client was actually associated. The NCS assumes the association started at the polling time which might be later than the actual association time. Therefore, the calculation of the average client throughput can give inaccurate results, especially for short client sessions.

- Protocol—802.11a/n or 802.11b/g/n.
- SSID—The user-defined Service Set Identifier name
- VLAN
- Vendor
- User Count
- Time Used (Minutes)
- Traffic (MB)
- Session Count
- % of Users
- % of Time
- % of Traffic
- % of Session
- Total Time of a session

Client Summary Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Client Summary report, depending on how the report is customized (see Figure 14-15):

Client Summary

- Number of Sessions (mandatory column)
- Number of Total Users (mandatory column)—Number of unique endpoints or MAC addresses.
- Number of Unique Users—Number of unique usernames that are authenticated.
- Number of New Users
- Number of Unique Access Points
- Number of Users per Access Point
- Total session time in minutes
- Total traffic (MB)
- Average traffic per session (KB) and per user (in KB)
- Total throughput (MBPS)
- Average throughput per session and per user (MBPS)

Note When the NCS does not receive client traps, it relies on client status polling to discover client associations (The task runs every 5 minutes by default). However, the NCS cannot accurately determine when the client was actually associated. The NCS assumes the association started at the polling time which might be later than the actual association time. Therefore, the calculation of the average client throughput can give inaccurate results, especially for short client sessions.

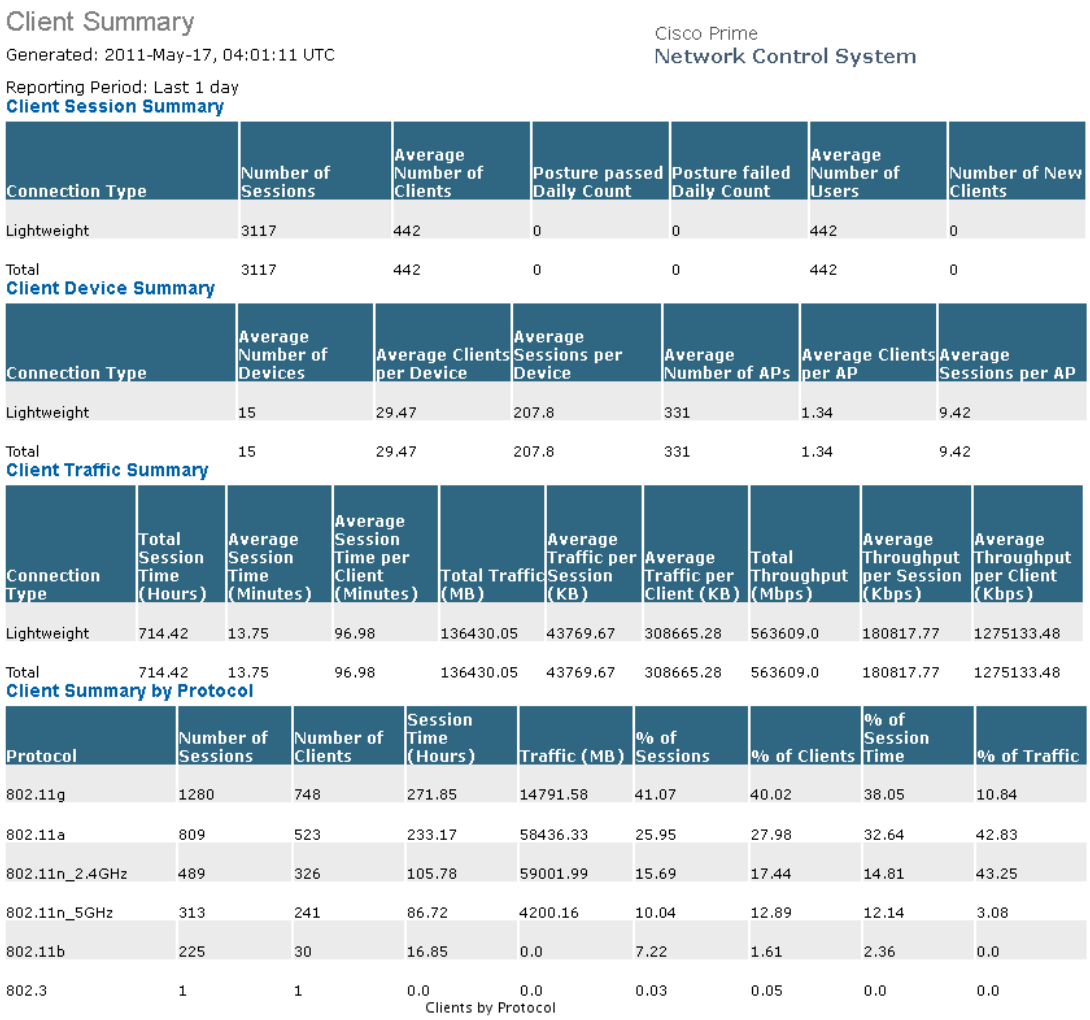
Note The NCS only counts authenticated sessions. If a user fails on DHCP or authentication, the NCS might not have a session for it. Also, the NCS considers every detected AP association as a session. For instance, if a client roams from one access point to another, the NCS can have two association sessions.

Client Summary by Protocol, SSID, VLAN, and Vendor:

- Protocol (mandatory column)
- SSID (mandatory column)
- VLAN (mandatory column)
- Vendor (mandatory column)
- User Count (mandatory column)
- Time Used (mandatory column)
- Traffic (mandatory column)
- Session Count (mandatory column)

- % of users, time, traffic, and sessions

Figure 14-15 Client Summary Report Results



Client Summary

Generated: 2011-May-17, 04:01:11 UTC

Cisco Prime
Network Control System

Reporting Period: Last 1 day

Client Session Summary

Connection Type	Number of Sessions	Average Number of Clients	Posture passed Daily Count	Posture failed Daily Count	Average Number of Users	Number of New Clients
Lightweight	3117	442	0	0	442	0
Total	3117	442	0	0	442	0

Client Device Summary

Connection Type	Average Number of Devices	Average Clients per Device	Average Sessions per Device	Average Number of APs	Average Clients per AP	Average Sessions per AP
Lightweight	15	29.47	207.8	331	1.34	9.42
Total	15	29.47	207.8	331	1.34	9.42

Client Traffic Summary

Connection Type	Total Session Time (Hours)	Average Session Time (Minutes)	Average Session Time per Client (Minutes)	Total Traffic (MB)	Average Traffic per Session (KB)	Average Traffic per Client (KB)	Total Throughput (Mbps)	Average Throughput per Session (Kbps)	Average Throughput per Client (Kbps)
Lightweight	714.42	13.75	96.98	136430.05	43769.67	308665.28	563609.0	180817.77	1275133.48
Total	714.42	13.75	96.98	136430.05	43769.67	308665.28	563609.0	180817.77	1275133.48

Client Summary by Protocol

Protocol	Number of Sessions	Number of Clients	Session Time (Hours)	Traffic (MB)	% of Sessions	% of Clients	% of Session Time	% of Traffic
802.11g	1280	748	271.85	14791.58	41.07	40.02	38.05	10.84
802.11a	809	523	233.17	58436.33	25.95	27.98	32.64	42.83
802.11n_2.4GHz	489	326	105.78	59001.99	15.69	17.44	14.81	43.25
802.11n_5GHz	313	241	86.72	4200.16	10.04	12.89	12.14	3.08
802.11b	225	30	16.85	0.0	7.22	1.61	2.36	0.0
802.3	1	1	0.0	0.0	0.03	0.05	0.0	0.0

Clients by Protocol

Client Traffic

This report displays the traffic by the wireless clients on your network.

Click **Client Traffic** from the Report Launch Pad to open the Client Traffic Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

Configuring a Client Traffic Report

This section describes how to configure a Client Traffic report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.

- Report by
  - All—Choose **All** if you want to monitor the traffic of all the clients in the network.
  - Controller IP Address—Choose **Controller IP Address** if you want to monitor the traffic of all or specific controller in the network.
  - Controller Host Name—Choose **Controller Host Name** if you want to monitor the traffic of all or specific controller in the network.
  - Autonomous AP IP Address—Choose **Autonomous AP IP Address** if you want to monitor the traffic of all autonomous access points in the network.
  - Autonomous AP Host Name—Choose **Autonomous AP Host Name** if you want to monitor the traffic of all autonomous access points in the network.
  - Switch IP Address—Choose **Switch IP Address** if you want to monitor the traffic of all switches in the network.
  - Switch Host Name—Choose **Switch Host Name** if you want to monitor the traffic of all switches in the network.
  - Floor Area—Choose **Floor Area** if you want to monitor the traffic of all the clients in a floor in the network.
  - Outdoor Area—Choose **Floor Area** if you want to monitor the traffic of all the clients in an outdoor area in the network.
  - AP by Floor Area—Choose **AP by Floor Area** if you want to monitor the traffic of all the access points in a floor in the network.
  - AP by Outdoor Area—Choose **AP by Outdoor Area** if you want to monitor the traffic of all the access points in an outdoor area in the network.
  - SSID—Choose **SSID** if you want if you want to monitor the traffic of all the clients in a network based on SSID.

Note This SSID also works as a second level filter if the report criteria is selected as not ALL. For example, if you choose Report By as Controller IP, Report Criteria as choose any controller, then the SSID filter becomes active and you can choose any SSID to run the report.

  - AP by RAP Mesh Role—Choose **AP by RAP Mesh Role** if you want to monitor the traffic of all the RAP Mesh access points in the network.
- Report Criteria—Either choose the corresponding option from the drop-down list, or click **Edit** to choose specific devices.The options vary based on the Report By option you chose.

Note In the Report Criteria page, click **Select** to confirm your sort criteria, or **Close** to return to the previous page.

- SSID—By default, this option is All SSIDs.
- Reporting Period—Specify the time period for which the report needs to be generated. You can choose from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

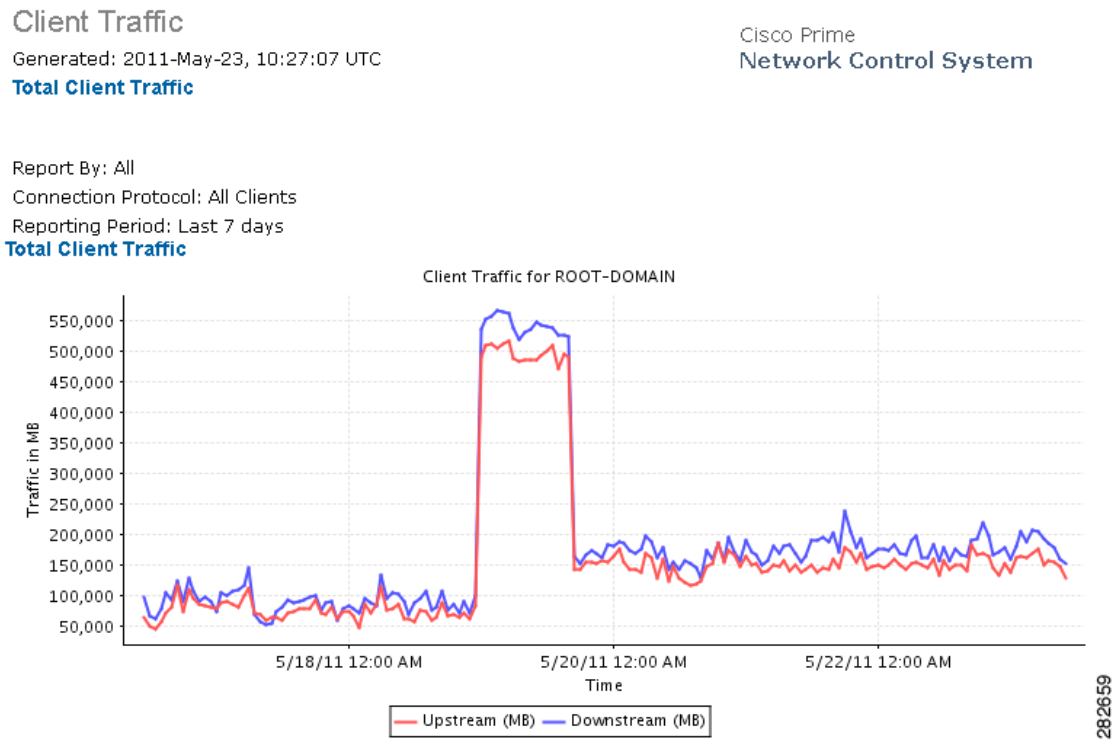
Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Client Traffic Report Results

Note Use the Customize Report Format to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The Figure 14-16 shows the potential results for a Client Traffic report, depending on how the report is customized.

Figure 14-16 Client Traffic Report Results



Client Traffic Stream Metrics

This report displays Traffic Stream Metrics for clients. You can select from the following:

- All clients of a given set of SSIDs
- All clients
- One specific client

Click **Client Traffic Stream Metrics** from the Report Launch Pad to open the Client Traffic Stream Metrics Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Client Traffic Stream Metrics Reports page.

Note The traffic stream metrics and radio performance background tasks must be running prior to generating this report.

Configuring a Client Traffic Stream Metrics Report

This section describes how to configure a Client Traffic Stream Metrics report.

Settings

The following settings can be configured for a Client Traffic Stream Metrics report:

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - SSID—Choose **All SSIDs** from the Report Criteria page, or click **Edit** to choose a specific or multiple SSIDs.
  - Client MAC Address—Choose **All Clients** from the Report Criteria page, or click **Edit** to choose specific clients.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - **Last**—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or client the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Client Traffic Stream Metrics report, depending on how the report is customized:

- Time (mandatory column)
- Client MAC (mandatory column)
- QoS (mandatory column)—QoS values (packet latency, packet jitter, packet loss, roaming time) which can affect how the WLAN are monitored. Access points and clients measure the metrics, access points collect the measurements and send them to the controller. The access points update the controller with traffic stream metric information every 90 seconds and 10 minutes of data is stored at one time.
- AP Name (mandatory column)
- Radio Type (mandatory column)
- Avg Queuing Delay (ms) (Downlink) (mandatory column)—Average queuing delay in milliseconds for the downlink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes the time for retries, if needed.
- Avg Queuing Delay (ms) (Uplink) (mandatory column)—Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for retries, if needed.
- % PLR (Downlink)—Percentage of packets lost on the downlink (access point to client) during the 90 second interval.
- % PLR (Uplink)—Percentage of packets lost on the uplink (client to access point) during the 90 second interval.
- % Packets > 40ms Queuing Delay (Uplink)—Percentage of queuing delay packets greater than 40 ms.
- % Packets 20ms-40ms Queuing Delay (Uplink)—Percentage of queuing delay packets between 20 ms and 40 ms.
- Roaming Delay—Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the he first packet is received from the new access point after a successful roam.
- Time—Time that the statistics were gathered from the access point(s).
- Client MAC—MAC address of the client. This shows a list of the clients evaluated during the most recent 90 second interval. The client could be a VoIP phone, laptop, or PDA and refers to any client attached to the access point collecting measurements.

Client Traffic Stream Metrics Report Results

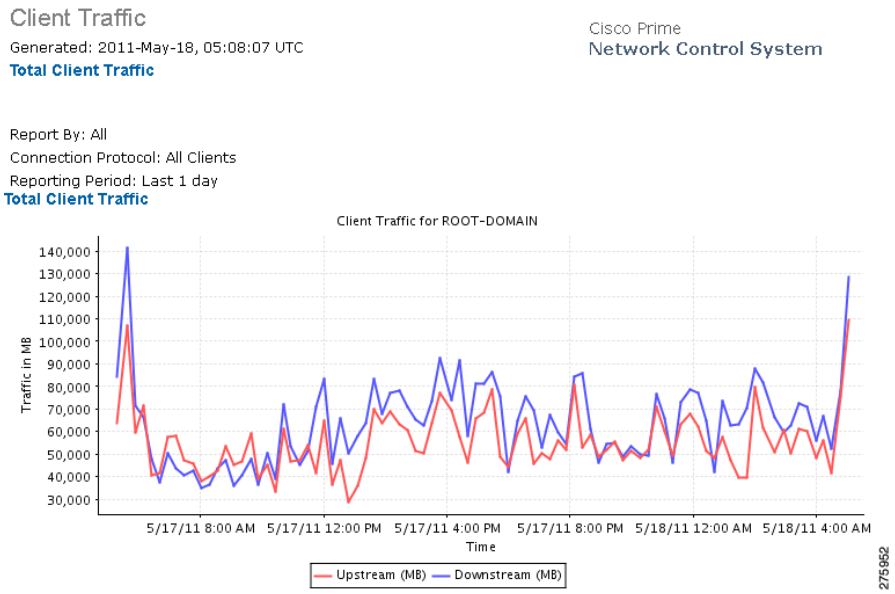
Note Use the Create Custom Report page to customize the displayed results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

The following are potential results for a Client Traffic Stream Metrics report, depending on how the report is customized (see Figure 14-17):

- Time (mandatory column)
- Client MAC (mandatory column)
- QoS (mandatory column)—QoS values (packet latency, packet jitter, packet loss, roaming time) which can affect the WLAN are monitored. Access points and clients measure the metrics, access points collect the measurements and send them to the controller. The access points update the controller with traffic stream metric information every 90 seconds and 10 minutes of data per client is stored in the WLC. The NCS polls this data and stores it for the last seven days.
- AP Name (mandatory column)
- Radio Type (mandatory column)
- Avg Queuing Delay (ms) (Downlink) (mandatory column)—Average queuing delay in milliseconds for the downlink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for retries, if needed.
- Avg Queuing Delay (ms) (Uplink) (mandatory column)—Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for retries, if needed.
- % PLR (Downlink)—Percentage of packets lost on the downlink (access point to client) during the 90 second interval.
- % PLR (Uplink)—Percentage of packets lost on the uplink (client to access point) during the 90 second interval.
- % Packets > 40ms Queuing Delay (Uplink)—Percentage of queuing delay packets greater than 40 ms.
- % Packets 20ms-40ms Queuing Delay (Uplink)—Percentage of queuing delay packets between 20ms-40 ms.
- Roaming Delay—Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the first packet is received from the new access point after a successful roam.
- Time—Time that the statistics were gathered from the access point(s).

Client MAC—MAC address of the client. This shows a list of the clients evaluated during the most recent 90 second interval. The client could be a VoIP phone, laptop, PDA and refers to any client attached to the access point collecting measurements.

Figure 14-17 Client Traffic Stream Metrics Report Results



Posture Status Count

This trending report displays the failed or succeeded client posture status count on your network.

This section contains the following topics:

- Configuring a Posture Status Count Report, page 14-61
- Posture Status Count Report Results, page 14-62

Configuring a Posture Status Count Report

This section describes how to configure a Posture Status Count report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.

– From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

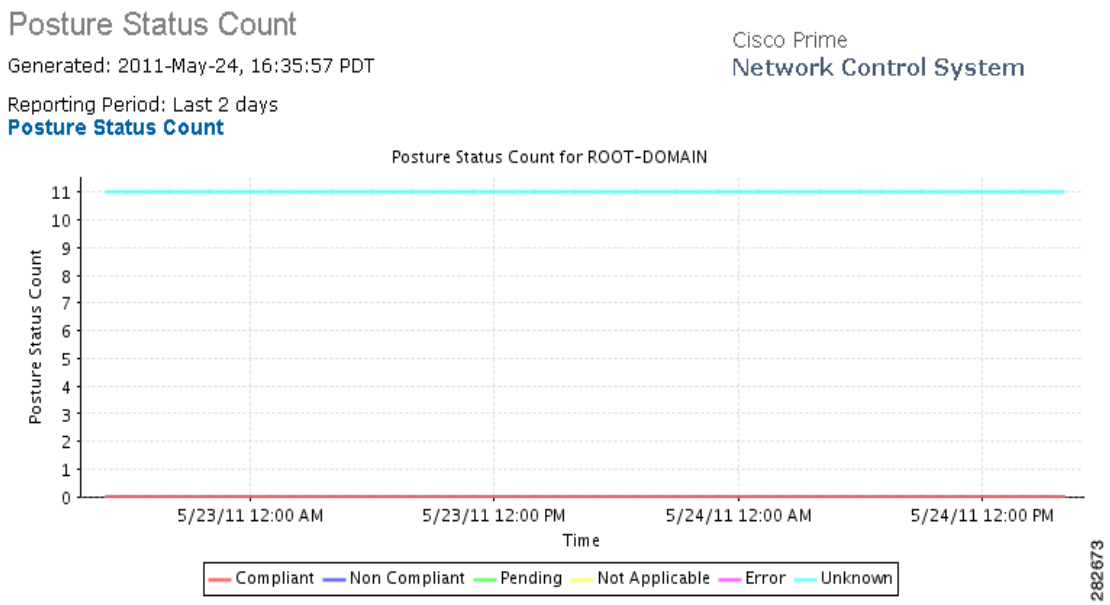
The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Posture Status Count Report Results

The Posture Status Count graph displays the following information (see Figure 14-18):

Figure 14-18 Posture Status Count Report



Throughput

This report displays the ongoing bandwidth used by the wireless clients on your network.

Note The Throughput report does not include wired clients or clients connected to autonomous Cisco IOS access points.

Click **Throughput** from the Report Launch Pad to open the Throughput Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

Note You cannot upgrade the Throughput reports to the NCS Release 1.0 and later.

Configuring a Throughput Report

This section describes how to configure a Throughput report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - All—Choose **All** if you want to monitor the traffic of all the clients in the network.
  - Controller IP Address—Choose **Controller IP Address** if you want to monitor the traffic of all or specific controller in the network.
  - Controller Host Name—Choose **Controller Host Name** if you want to monitor the traffic of all or specific controller in the network.
  - Autonomous AP IP Address—Choose **Autonomous AP IP Address** if you want to monitor the traffic of all autonomous access points in the network.
  - Autonomous AP Host Name—Choose **Autonomous AP Host Name** if you want to monitor the traffic of all autonomous access points in the network.
  - Switch IP Address—Choose **Switch IP Address** if you want to monitor the traffic of all switches in the network.
  - Switch Host Name—Choose **Switch Host Name** if you want to monitor the traffic of all switches in the network.
  - Floor Area—Choose **Floor Area** if you want to monitor the traffic of all the clients in a floor in the network.
  - Outdoor Area—Choose **Floor Area** if you want to monitor the traffic of all the clients in an outdoor area in the network.
  - AP by Floor Area—Choose **AP by Floor Area** if you want to monitor the traffic of all the access points in a floor in the network.
  - AP by Outdoor Area—Choose **AP by Outdoor Area** if you want to monitor the traffic of all the access points in an outdoor area in the network.
  - SSID—Choose **SSID** if you want if you want to monitor the traffic of all the clients in a network based on SSID.

  - AP by RAP Mesh Role—Choose **AP by RAP Mesh Role** if you want to monitor the traffic of all the RAP Mesh access points in the network.

- Report Criteria—Either choose the corresponding option from the drop-down list, or click **Edit** to choose specific devices.The options vary based on the Report By option you had chosen.

Note In the Report Criteria page, click **Select** to confirm your sort criteria or **Close** to return to the previous page.

- Connection Protocol—Choose **All Clients** or a specific radio type from the drop-down list.

Note Wired clients and clients associated to Cisco IOS access points are not included as part of this report.

- SSID—By default this option is All SSIDs.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

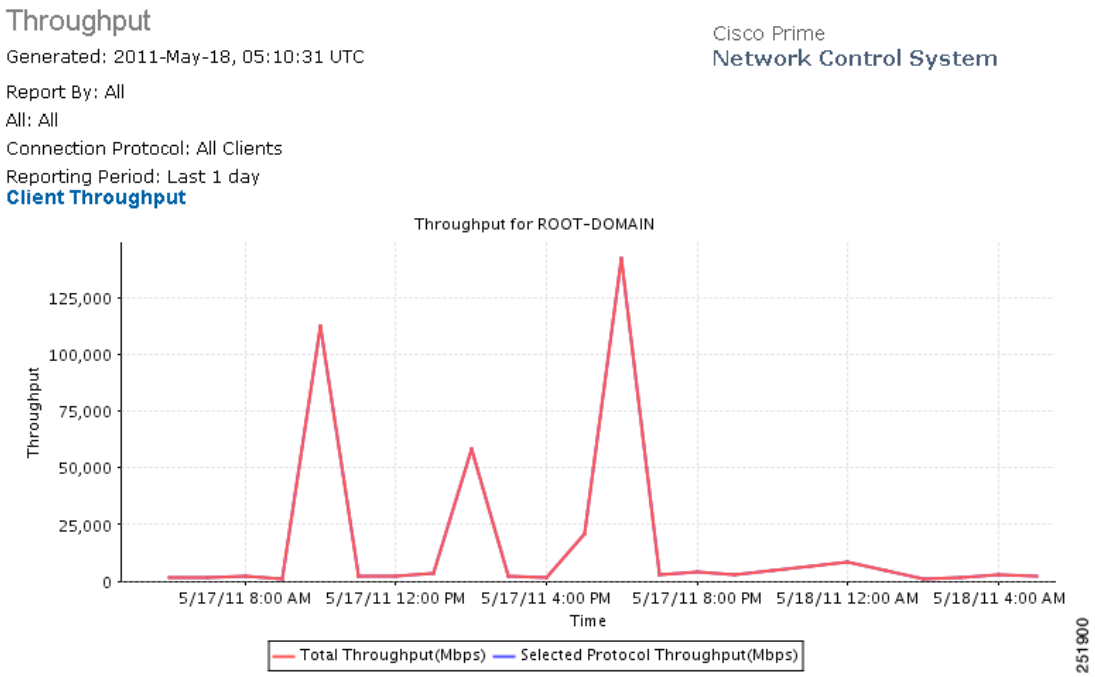
If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Throughput Report Results

The Throughput report graph displays the following (also see Figure 14-19):

- Total throughput (mbps)
- Throughput for the selected protocol
- Date and time for each indicated throughput level

Figure 14-19 Throughput Report Results



Unique Clients

This report displays all unique clients by the time, protocol, and controller filters that you select. A unique client is determined by the MAC address of the client device. These clients are sorted by controller in this report.

Click **Unique Clients** from the Report Launch Pad to open the Unique Clients Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

A new First Seen column is added in Release 6.0. It is the time that the NCS first learned of the client MAC address. For existing clients, the NCS sets the First Seen column with the timestamp currently in the database, which is the time the record was last updated.

Note The Unique Client report covers any client that started the connection during the specified time period or ended the connection during the specified time period or connected during the specified time period. The specified time period refers to the reporting period that you specify while scheduling the report.

Note Unique Clients reports do *not* include autonomous clients.

Configuring a Unique Clients Report

This section describes how to configure a Unique Clients report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - Controller—Choose **All Controllers** from the Report Criteria page, or click **Edit** to choose specific devices.
  - Floor Area—Choose **All Campuses > All Buildings > All Floors** from the Report Criteria page, or click **Edit** to choose specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Areas** from the Report Criteria page, or click **Edit** to choose specific locations.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All APs** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - SSID—Choose **All SSIDs** from the Report Criteria page, or click **Edit** to choose a specific or multiple SSIDs.
  - AP by RAP Mesh Role—Choose **All RAP APs** from the Report Criteria page, or click **Edit** to choose a specific RAP access point.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Connection Protocol—Choose **All Clients**, **Wired Clients**, or a specific radio type from the drop-down list.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Mandatory columns are displayed in blue font and cannot be moved to the Available data fields column. Last Seen, User, and MAC address are mandatory columns for the Unique Client report.

The following information is available on the unique client report:

- Host Name
- AP MAC Address
- IP Address—The IP address of the controller to which this client is associated.
- Controller IP Address
- Port
- Global Unique—The aggregate global unicast address of an IPv6 address. This field is populated only if a client is assigned a global unique IPv6 address.
- Local Unique—The local unicast address of an IPv6 address. This field is populated only if a client is assigned a local unique IPv6 address.
- Link Local—The link local unicast address of an IPv6 address. This field is populated only if a client is assigned a link local IPv6 address.
- Last Session Length
- VLAN ID—The VLAN Identifier. The range is 1 to 4096.
- CCX—The Cisco Client Extension version number.
- E2E
- Vendor—The vendor name for this client.
- IP Address—The IP address of the client. This field displays IPv6 address for IPv6 clients and IPv4 address for IPv4 and dual stack clients.
- AP Name—The access point to which this client is associated.
- Controller—The name of the controller to which this client is associated.
- 802.11 State—Client association status.
- SSID—The SSID to which this client is associated.
- Profile—The name of the profile to which this client is associated.
- Authenticated
- Protocol—802.11a, 802.11b, 802.11g, 802.11n_5 GHz, or 802.11b_2.4 GHz.
- Map Location

Unique Client Report Results

The following information is displayed for a Unique Client report (see Figure 14-20):

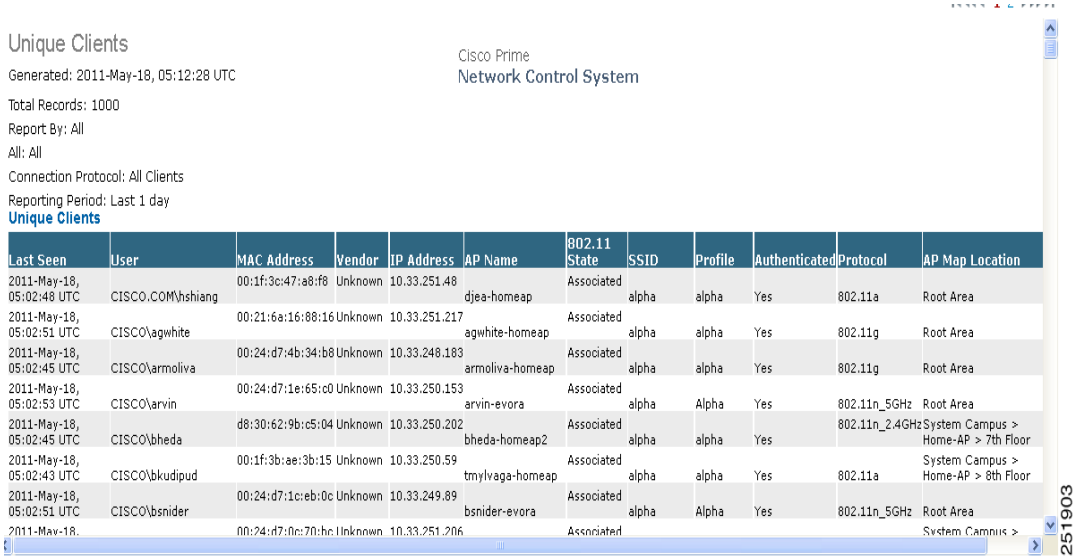
- First/Last Seen—Date and time the unique client was first and last viewed
- User—Client username
- Vendor—The vendor name or Unknown
- Client IP Address and MAC Address

- AP Name
- Controller—The controller to which the client was associated
- Port
- 802.11 State—Associated, Disassociated, or Idle
- SSID

Note N/A might appear in the SSID field if the client is probing.

- Authenticated—Indicates whether or not the client is authenticated (Yes or No).
- Protocol—802.11a, 802.11b, 802.11g, 802.11n_5GHz, or 802.11b_2.4GHz.
- VLAN ID
- CCX—Indicates whether or not CCX (Cisco Client Extensions) is supported.
- E2E—Indicates whether or not E2E (End to End) is supported.
- Map Location

Figure 14-20 Unique Client Report Results



Last Seen	User	MAC Address	Vendor	IP Address	AP Name	802.11 State	SSID	Profile	Authenticated	Protocol	AP Map Location
2011-May-18, 05:02:48 UTC	CISCO.COM\hshiang	00:1f:3c:47:a8:f8	Unknown	10.33.251.48	djea-homeap	Associated	alpha	alpha	Yes	802.11a	Root Area
2011-May-18, 05:02:51 UTC	CISCO\agwhite	00:21:6a:16:88:16	Unknown	10.33.251.217	agwhite-homeap	Associated	alpha	alpha	Yes	802.11g	Root Area
2011-May-18, 05:02:45 UTC	CISCO\armoliva	00:24:d7:4b:34:b8	Unknown	10.33.248.183	armoliva-homeap	Associated	alpha	alpha	Yes	802.11g	Root Area
2011-May-18, 05:02:53 UTC	CISCO\arvin	00:24:d7:1e:65:c0	Unknown	10.33.250.153	arvin-evora	Associated	alpha	Alpha	Yes	802.11n_5GHz	Root Area
2011-May-18, 05:02:45 UTC	CISCO\bheda	d8:30:62:9b:c5:04	Unknown	10.33.250.202	bheda-homeap2	Associated	alpha	alpha	Yes	802.11n_2.4GHz	System Campus > Home-AP > 7th Floor
2011-May-18, 05:02:43 UTC	CISCO\bkudipud	00:1f:3b:ae:3b:15	Unknown	10.33.250.59	tmylvaga-homeap	Associated	alpha	alpha	Yes	802.11a	System Campus > Home-AP > 8th Floor
2011-May-18, 05:02:51 UTC	CISCO\bsnider	00:24:d7:1c:eb:0c	Unknown	10.33.249.89	bsnider-evora	Associated	alpha	Alpha	Yes	802.11n_5GHz	Root Area
2011-May-18,		00:24:d7:0c:70:bc	Unknown	10.33.251.206		Associated					System Campus >

CCX Client Statistics

This report displays the 802.11 and security statistics for Cisco Compatible Extensions v5 clients or Cisco Compatible Extensions v6 clients depending upon the options you choose to run the report.

Click **CCX Client Statistics** from the Report Launch Pad to open the CCX Client Statistics Report page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

Configuring a CCX Client Statistics Report

This section describes how to configure a CCX Client Statistics report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- CCX—Choose **All**, **V5**, or **V6** from the drop-down list.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

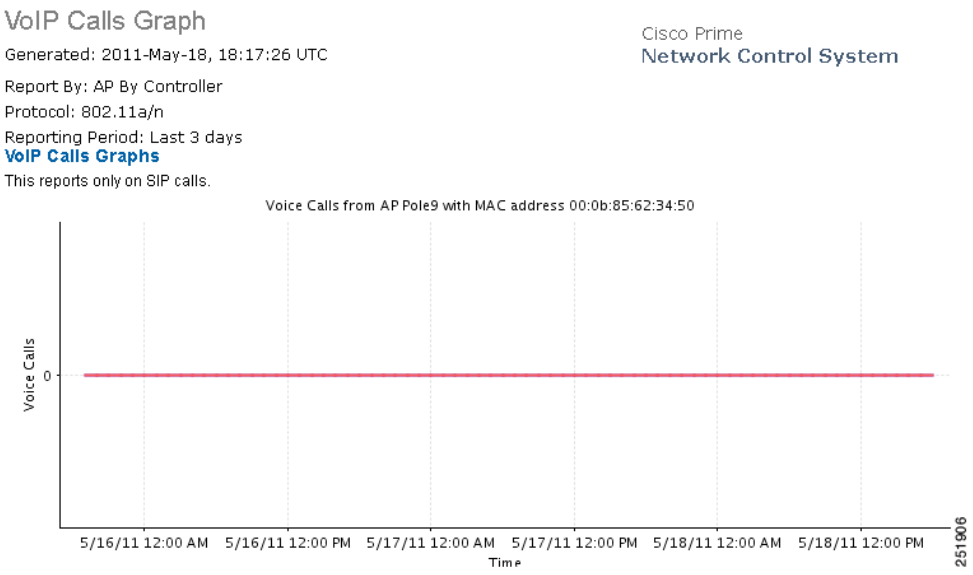
CCX Client Statistics Report Results

The following information is displayed for the CCX Client Statistics report (see Figure 14-21):

- Client MAC Address
- Transmitted Fragment Count—This counter increments for each successfully received MPDU Data or Management type.
- Multicast Transmitted Frame Count—This counter increments only when the multicast bit is set in the destination MAC address of a successfully transmitted MAC Service Data Unit (MSDU). When operating as a Station (STA) in an Extended Service Set (ESS), where these frames are directed to the access point, this implies having received an acknowledgment to all associated MAC Protocol Data Units (MPDUs).
- Failed Count—This counter increments when an MSDU is unsuccessfully transmitted.
- Retry Count—This counter increments when an MSDU is successfully transmitted after one or more retransmissions.
- Multicast Retry Count—This counter increments when an MSDU is successfully transmitted after more than one retransmission.
- Frame Duplicate Count—This counter increments when a frame is received that the Sequence Control field indicates is a duplicate.
- RTS Success Count—This counter increments when a CTS (clear-to-send) is received in response to an RTS (ready-to-send).
- RTS Fail Count—This counter increments when a clear-to-send is not received in response to a ready-to-send.

- ACK Fail Count—This counter increments when an ACK is not received when expected.
- Received Fragment Count—The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
- Multicast Received Frame Count—This counter increments when an MSDU is received with the multicast bit set in the destination MAC address.
- FCS Error Count—This counter increments when an Frame Check Sequence error is detected in a received MPDU.
- Transmitted Frame Count—This counter increments for each successfully transmitted MSDU.

Figure 14-21 CCX Client Statistics Report Results



Compliance Reports

The Configuration Audit report displays the differences between the NCS and its controllers. The PCI DSS Compliance report summarizes your Wireless LAN Security components with reference to the Payment Card Industry (PCI) Data Security Standard (DSS) requirements. PCI DSS compliance is required for all merchants and service providers that store, process, or transmit cardholder data. You can find PCI DSS standards at the PCI Security Standards Council website.

The section describes the Compliance Reports available and contains the following topics:

- Configuration Audit, page 14-71
- PCI DSS Detailed, page 14-74
- PCI DSS Summary, page 14-76

Configuration Audit

This report displays the configuration differences between the NCS and its controllers. You must configure audit mode on the Administration > Settings page. In audit mode, you can perform an audit based on templates or the stored configuration. The report shows the last time an audit was performed using the Configuration Sync background task.

Click **Configuration Audit** from the Report Launch Pad to open the Configuration Audit Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Configuration Reports page. See the "Configuring a Configuration Audit Report" section on page 14-71 and the "Configuration Audit Report Results" section on page 14-72 for more information.

Configuring a Configuration Audit Report

This section describes how to configure a Configuration Audit report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Controller—Choose **All Controllers** or a specific controller from the available list.
- Audit Time—Choose **Latest** or a specific date and time from the available list.

Note The available audit times are based on when the Configuration Sync background task was run.

- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Note A Configuration Audit report contains the following sections: Audit Summary, Applied Templates and Config Group Template Discrepancies, Enforced Values, Failed Enforcements, and the NCS Config Discrepancies. Choose the applicable report from the Customizable Report drop-down list.
To customize report results for a particular section, choose the applicable section from the Customizable Report drop-down list.

A Configuration Audit report contains the following default information, depending on which customized report is selected:

- Controller Name
- Audit Status
- Audit Time
- Name
- Audit Object Display Name
- Device Sync State
- Time
- Client MAC Address
- IP Address
- Message
- Description
- Attribute
- Attribute Value in the NCS
- Attribute Value in Device
- Enforced Value
- Instance Name
- Description
- Error Message
- Attribute Value in DB

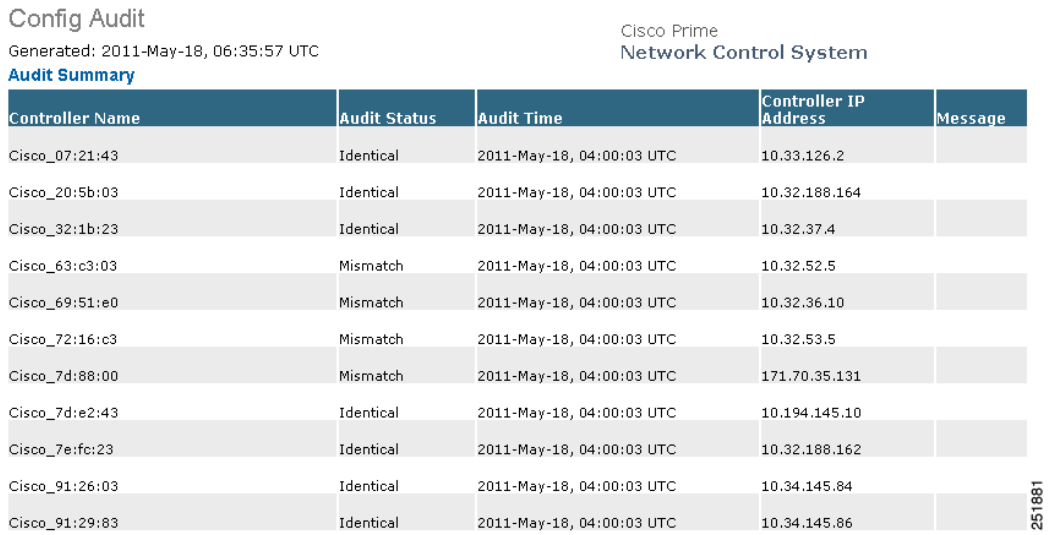
Configuration Audit Report Results

The following are potential results for a Configuration Audit report, depending on how the report is customized (see Figure 14-22):

- Audit Summary results
  - Controller Name (mandatory column)
  - Audit Status (mandatory column)—Not Available (no audit occurred on this switch), Identical (no configuration differences were discovered), Mismatch (configuration differences were discovered).

  - Audit Time (mandatory column)—The time when the network audit background task was run via Configuration Sync task.
  - IP Address—The IP address of the audited controller.
  - Message—It reports “Device unreachable” if the device is unreachable. Also, if any exceptions is found during the audit, it reports “Internal Exception, check the log files”.
- Applied Templates and Config Group Template Discrepancies results
  - Name (mandatory column)
  - Template Name (mandatory column)
  - Audit Status (mandatory column)—(Mismatch, Identical, Not Available).
  - Template Applied Via—Template description.
  - Attribute
  - NCS Value
  - Controller Device
- Enforced Values results
  - Name (mandatory column)
  - Template Name (mandatory column)
  - Audit Status (mandatory column)
  - Template Applied Via
  - Attribute
  - Enforced Value
  - Controller Value
- Failed Enforcements results
  - Name (mandatory column)
  - Object Name
  - Description
  - Error Message
- NCS Config Discrepancies results
  - Controller Name (mandatory column)
  - Object Name (mandatory column)
  - Audit Status (mandatory column)
  - Attribute (mandatory column)
  - NCS Value
  - Controller Value

Figure 14-22 Configuration Audit Report Results



Config Audit

Generated: 2011-May-18, 06:35:57 UTC

Cisco Prime
Network Control System

Audit Summary

Controller Name	Audit Status	Audit Time	Controller IP Address	Message
Cisco_07:21:43	Identical	2011-May-18, 04:00:03 UTC	10.33.126.2	
Cisco_20:5b:03	Identical	2011-May-18, 04:00:03 UTC	10.32.188.164	
Cisco_32:1b:23	Identical	2011-May-18, 04:00:03 UTC	10.32.37.4	
Cisco_63:c3:03	Mismatch	2011-May-18, 04:00:03 UTC	10.32.52.5	
Cisco_69:51:e0	Mismatch	2011-May-18, 04:00:03 UTC	10.32.36.10	
Cisco_72:16:c3	Mismatch	2011-May-18, 04:00:03 UTC	10.32.53.5	
Cisco_7d:88:00	Mismatch	2011-May-18, 04:00:03 UTC	171.70.35.131	
Cisco_7d:e2:43	Identical	2011-May-18, 04:00:03 UTC	10.194.145.10	
Cisco_7e:fc:23	Identical	2011-May-18, 04:00:03 UTC	10.32.188.162	
Cisco_91:26:03	Identical	2011-May-18, 04:00:03 UTC	10.34.145.84	
Cisco_91:29:83	Identical	2011-May-18, 04:00:03 UTC	10.34.145.86	

251881

PCI DSS Detailed

This report displays in detail, the PCI Data Security Standard (DSS) Version 2.0 requirements that are relevant to your wireless network security.

Click **PCI DSS Detailed** from the Report Launch Pad to open the PCI DSS Detailed Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the PCI DSS Detailed Reports page. See the "Configuring a PCI DSS Detailed Report" section on page 14-74 and the "PCI DSS Detailed Report Results" section on page 14-75 for more information.

Configuring a PCI DSS Detailed Report

This section describes how to configure a PCI DSS Detailed report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By

- Controller—Choose **All Controllers** from the Report Criteria list, or click **Edit** to choose specific devices.
- MSE—Choose **All MSEs** from the Report Criteria list, or click **Edit** to choose a specific MSE.
- Floor Area—Choose **All Campuses > All Buildings > All Floors** from the Report Criteria list, or click **Edit** to choose specific locations.

Note In the Filter Criteria list, choose the appropriate filter criteria.

- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

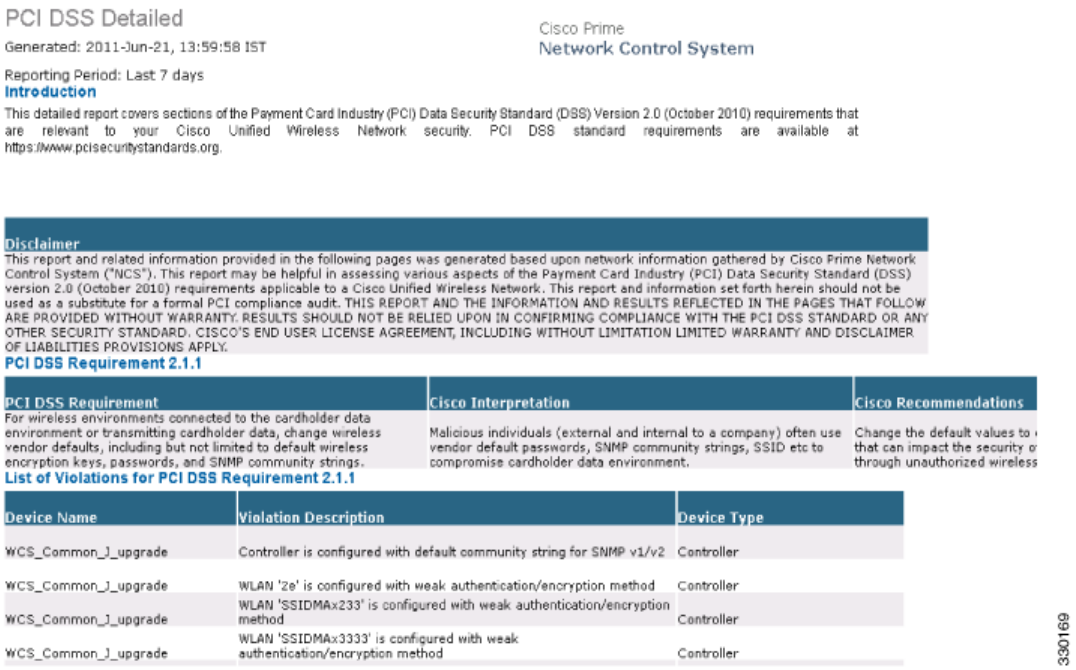
Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

PCI DSS Detailed Report Results

The following are the results for a PCI DSS Detailed report (see Figure 14-23):

Figure 14-23 PCI DSS Detailed Report



PCI DSS Detailed

Generated: 2011-Jun-21, 13:59:58 IST

Cisco Prime
Network Control System

Reporting Period: Last 7 days

Introduction

This detailed report covers sections of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 2.0 (October 2010) requirements that are relevant to your Cisco Unified Wireless Network security. PCI DSS standard requirements are available at https://www.pcisecuritystandards.org.

Disclaimer

This report and related information provided in the following pages was generated based upon network information gathered by Cisco Prime Network Control System ("NCS"). This report may be helpful in assessing various aspects of the Payment Card Industry (PCI) Data Security Standard (DSS) version 2.0 (October 2010) requirements applicable to a Cisco Unified Wireless Network. This report and information set forth herein should not be used as a substitute for a formal PCI compliance audit. THIS REPORT AND THE INFORMATION AND RESULTS REFLECTED IN THE PAGES THAT FOLLOW ARE PROVIDED WITHOUT WARRANTY. RESULTS SHOULD NOT BE RELIED UPON IN CONFIRMING COMPLIANCE WITH THE PCI DSS STANDARD OR ANY OTHER SECURITY STANDARD. CISCO'S END USER LICENSE AGREEMENT, INCLUDING WITHOUT LIMITATION LIMITED WARRANTY AND DISCLAIMER OF LIABILITIES PROVISIONS APPLY.

PCI DSS Requirement 2.1.1

PCI DSS Requirement	Cisco Interpretation	Cisco Recommendations
For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	Malicious individuals (external and internal to a company) often use vendor default passwords, SNMP community strings, SSID etc to compromise cardholder data environment.	Change the default values to that can impact the security o through unauthorized wireless

List of Violations for PCI DSS Requirement 2.1.1

Device Name	Violation Description	Device Type
WCS_Common_1_upgrade	Controller is configured with default community string for SNMP v1/v2	Controller
WCS_Common_1_upgrade	WLAN '2e' is configured with weak authentication/encryption method	Controller
WCS_Common_1_upgrade	WLAN 'SSIDMAx233' is configured with weak authentication/encryption method	Controller
WCS_Common_1_upgrade	WLAN 'SSIDMAx3333' is configured with weak authentication/encryption method	Controller

330169

PCI DSS Summary

This report displays the summarized PCI Data Security Standard (DSS) Version 2.0 requirements that are relevant to your wireless network security.

Click **PCI DSS Summary** from the Report Launch Pad to open the PCI DSS Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the PCI DSS Summary Reports page. See the "Configuring a PCI DSS Summary Report" section on page 14-76 and the "PCI DSS Summary Report Results" section on page 14-77 for more information.

Configuring a PCI DSS Summary Report

This section describes how to configure a PCI DSS Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

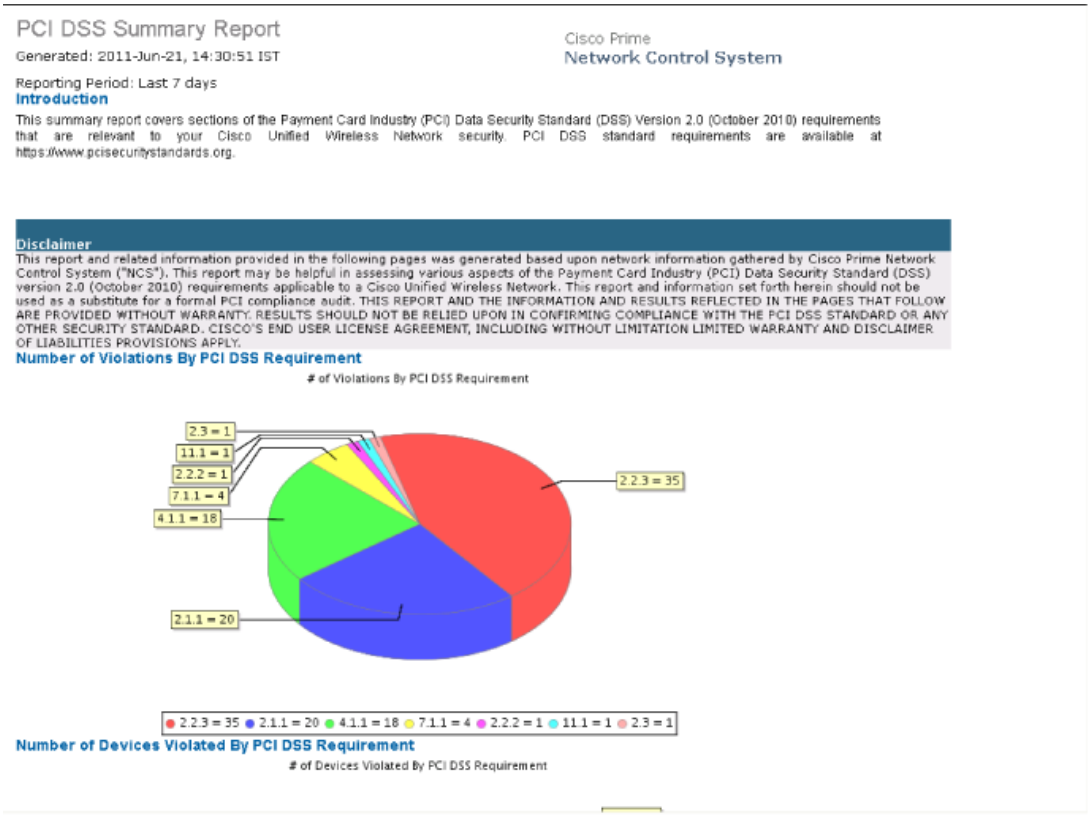
Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

PCI DSS Summary Report Results

The results of PCI DSS Summary report contain the following information (see Figure 14-24 for a snippet):

- Number of Violations By PCI DSS Requirement
- Number of Devices Violated By PCI DSS Requirement
- Summary By PCI DSS Requirement
- Summary By Devices
- List of Violations

Figure 14-24 PCI DSS Summary Report



ContextAware Reports

This section describes the various ContextAware reports that you can generate through the NCS Reports Launch Pad.

To generate a new ContextAware report, click **New** next to a ContextAware report type to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

This section describes the ContextAware reports you can create and contains the following topics:

Client Location History

This report displays location history of a wireless client detected by an MSE.

This section contains the following topics:

Configuring a Client Location History

This section describes how to configure a Client Location History report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - Client MAC address.
- Report Criteria—Click **Edit** and enter a valid MAC address as the filter criteria.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and choose a period of time from the drop-down list.

    Or
  - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Client Location History Results

The results of the Client Location History report contain the following information:

- Last Located—The place at which the client was last located.
- Client Location—The current position of the client.
- MSE—The name of the MSE to which the client is associated with.
- User—The username of the client.
- Detecting Controllers—The IP address of the detecting controller.
- 802.11 State—The state of 802.11. It could be either Probing.
- IP Address—The IP address of the client.
- AP MAC Address—The MAC address of the associated access point.
- Authenticated—Whether authenticated or not. This could be either Yes or No.
- SSID—The SSID used by the client.
- Protocol—The protocol used to retrieve the information from the client.

Client Location Tracking

This report displays wireless clients and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

- Configuring a Client Location Tracking, page 14-80
- Client Location Tracking Results, page 14-81

Configuring a Client Location Tracking

This section describes how to configure a Client Location Tracking report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - MSE By Floor Area.
  - MSE By Outdoor Area
  - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and choose the required filter criteria.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and choose a period of time from the drop-down list.

    Or
  - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Client Location Tracking Results

The results of the Client Location Tracking report contain the following information:

- Last Located—The place where the client was last located.
- MAC Address—The MAC address of the client.
- Client Location—The current location of the client.
- MSE—The name of the MSE to which the client is associated with.
- User—The username of the client.
- Detecting Controllers—The IP address of the detecting controller.
- 802.11 State—The state of 802.11. It could be either Probing.
- IP Address—The IP address of the client.
- SSID—The SSID used by the client.
- Protocol—The protocol used to retrieve the information from the client.

Guest Location Tracking

This report displays Guest clients and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

Configuring a Guest Location Tracking

This section describes how to configure a Guest Location Tracking report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - MSE By Floor Area.
  - MSE By Outdoor Area
  - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and choose the required filter criteria.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and choose a period of time from the drop-down list.

    Or
  - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Guest Location Tracking Results

The results of the Guest Location Tracking report contain the following information:

- Last Located—The place where the guest client was last located.
- Guest Username—The login name of the guest client user.
- MAC Address—The MAC address of the guest client.
- Guest Location—The current location of the guest client.
- MSE—The name of the MSE to which the guest client is associated with.
- Detecting Controllers—The IP address of the detecting controller.
- IP Address—The IP address of the guest client.
- AP MAC Address—The MAC address of the access point to which the guest client is associated with.
- SSID—The SSID used by the guest clients.
- Protocol—The protocol used to retrieve the information from the guest client.

Location Notifications

This report displays Context Aware Notifications generated by MSEs.

This section contains the following topics:

- Configuring a Location Notification, page 14-83
- Location Notification Results, page 14-84

Configuring a Location Notification

This section describes how to configure a Location Notification report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - Missing Device Notifications by MSE
  - Missing Device Notifications by Floor Area
  - Missing Device Notifications by Outdoor Area
  - Device In/Out Notifications by MSE
  - Device In/Out Notifications by Floor Area
  - Device In/Out Notifications by Outdoor Area
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and choose the required filter criteria.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Device Type
  - All
  - Client
  - Tag
  - Rogue Client
  - Rogue AP
  - Interferer
- Reporting Period
  - Select the radio button and choose a period of time from the drop-down list.

    Or
  - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Location Notification Results

The results of Location Notification report contain the following information:

- Last Seen—The date and time when the device was last located.
- MAC Address—The MAC address of the device.
- Device Type—The type of the device.
- Asset Name—The name of the asset.
- Asset Group—The name of the asset group.
- Asset Category—The name of the asset category.

- Map Location—The map location where the device was located.
- serverName—The name of the server that sends the ContextAware notifications.

Rogue AP Location Tracking

This report displays Rogue access points and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

Configuring a Rogue AP Location Tracking

This section describes how to configure a Rogue AP Location Tracking report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - MSE By Floor Area.
  - MSE By Outdoor Area
  - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and choose the required filter criteria.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and choose a period of time from the drop-down list.

    Or
  - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Rogue AP Location Tracking Results

The results of the Rogue AP Location Tracking report contain the following information:

- Last Located—The place where the rogue access point was last located.
- MAC Address—The MAC address of the rogue access point.
- Rogue AP Location—The current location of the rogue access point.
- MSE—The name of the MSE to which the rogue access point is associated with.
- State—The state of the location tracking. This could be either Alert or Pending.

Rogue Client Location Tracking

This report displays Rogue Client access points and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

Configuring a Rogue Client Location Tracking

This section describes how to configure a Rogue Client Location Tracking report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - MSE By Floor Area.
  - MSE By Outdoor Area
  - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and choose a period of time from the drop-down list.

Or

– Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Rogue Client Location Tracking Results

The results of Rogue Client Location Tracking report contain the following information:

- Last Located—The place where the client was last located.
- MAC Address—The MAC address of the rogue client.
- Rogue Client Location—The current location of the rogue client.
- MSE—The name of the MSE to which the rogue client is associated with.
- Rogue AP—The rogue access point to which the rogue client is associated with.
- Detecting Controllers—The IP address of the detecting controller.
- State—The state of the location tracking. This could be either Alert or Pending.

Tag Location History

This report displays Location history of a tag detected by an MSE.

This section contains the following topics:

Configuring a Tag Location History

This section describes how to configure a Tag Location History report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - Tag MAC address.
- Report Criteria—Click **Edit** and enter a valid Tag MAC address as the filter criteria.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and choose a period of time from the drop-down list.

    Or
  - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Tag Location History Results

The results of Tag Location History report contain the following information:

- Last Located—The place at which the tag was last located.
- Tag Location—The current location of the tag.
- MSE—The name of the MSE to which this client is associated with.
- Detecting Controller—The IP address of the detecting controller.
- Vendor—The name of the vendor for the client.
- Battery Status—The battery status of the client.

Tag Location Tracking

This report displays tags and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

Configuring a Tag Location Tracking

This section describes how to configure a Tag Location Tracking report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - MSE By Floor Area.
  - MSE By Outdoor Area
  - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Select the radio button and choose a period of time from the drop-down list.

    Or
  - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Tag Location Tracking Results

The results of the Tag Location Tracking report contain the following information:

- Last Located—The place at which the tag was last located.
- Tag Location—The current location of the tag.
- MSE—The name of the MSE to which this client is associated with.
- Detecting Controller—The IP address of the detecting controller.
- Vendor—The name of the tag vendor.
- Battery Status—The status of the battery of that tag.

Device Reports

Click **New** for a Device report type to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

This section describes the device reports you can create and contains the following topics:

AP Image Predownload

This report displays scheduled download software task status.

Click **AP Image Predownload** from the Report Launch Pad to open the AP Image Predownload page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the AP Image Predownload Reports page. See the "Configuring an AP Image Predownload Report" section on page 14-91 and the "AP Image Predownload Report Results" section on page 14-92 for more information.

Configuring an AP Image Predownload Report

This section describes how to configure a AP Image Predownload report.

Settings

The following settings can be configured for a AP Image Predownload report:

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose specific devices.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose specific locations or devices.

Note In the Report Criteria page, you can choose **All Access Points** or **All OfficeExtend Access Points**.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Creating a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Export Now—Click to export the report results. The supported export formats is PDF and CSV.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

AP Image Predownload Report Results

The following are potential results for an AP Image Predownload report, depending on how the report is customized:

- AP Name—Access point name.
- Primary Image—Current Primary Image present in the AP.
- Backup Image—Current Backup Image present in the AP.
- Predownload Version—The image version that is currently downloading to the AP from the controller as part of the predownload process.
- Predownload Status—The current status of the image download as part of the predownload process.
- MAC Address—MAC Address of the AP.
- Controller IP Address—IP address of the controller to which the access point is associated.
- Upgrade Role—The current status of the upgrade role. It could be any of the following:
  - Master Central
  - Master Local
  - Slave Central
  - Slave Local
  - Unknown

AP Profile Status

This report displays access point load, noise, interference, and coverage profile status.

Click **AP Profile Status** from the Report Launch Pad to open the AP Profile Status Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the AP Profile Status Reports page. See the "Configuring an AP Profile Report" section on page 14-93 and the "AP Profile Status Report Results" section on page 14-94 for more information.

Configuring an AP Profile Report

This section describes how to configure an AP Profile report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose specific devices.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose specific locations or devices.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose specific locations or devices.

Note In the Reports Criteria page, you can choose **All Access Points** or All OfficeExtend Access Points.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

AP Profile Status report results include the following:

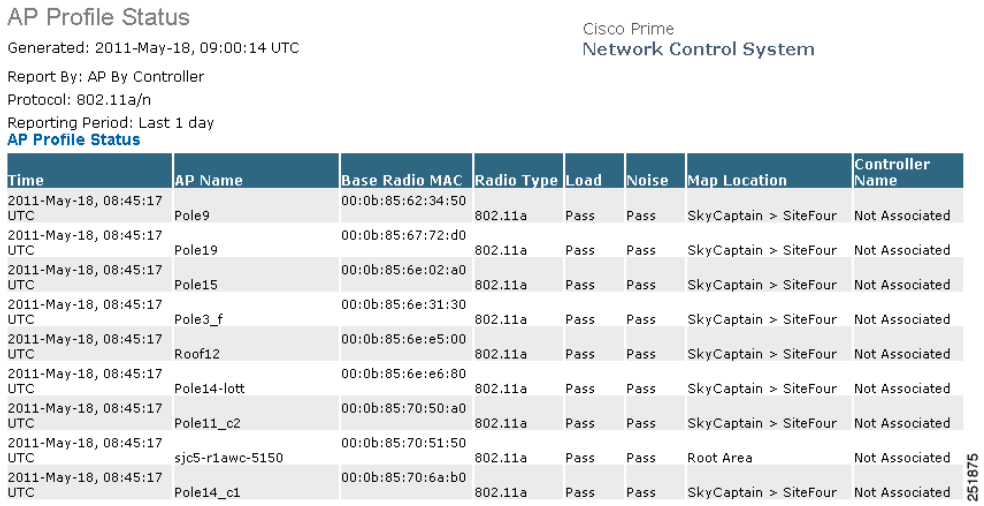
- Time—The date and time at which AP Profile Status is collected.
- AP Name—The access point name.
- AP MAC address—The MAC address of the access point.
- Radio Type—802.11a/n or 802.11b/g/n.
- Load—*True* if the load level exceeds a threshold level, otherwise *false*.
- Noise—*True* if the noise level exceeds a threshold level, otherwise *false*.
- Controller Name—The controller to which the access point is associated.
- Interference—*True* if the interference level exceeds a threshold level, otherwise *false*.
- Coverage—*True* if the coverage level exceeds a threshold level, otherwise *false*.
- Controller IP Address—The IP address of the controller to which the access point is associated.

AP Profile Status Report Results

The following are potential results for an AP Profile Status report, depending on how the report is customized (see Figure 14-25):

- Time (mandatory column)—The date and time at which AP Profile Status is collected.
- AP Name (mandatory column)—Access point name.
- AP MAC address—MAC address of the access point.
- Radio Type—802.11a/n or 802.11b/g/n.
- Load—Pass or Fail. Indicates whether or not the load level exceeds a threshold level.
- Noise—Pass or Fail. Indicates whether or not the noise level exceeds a threshold level.
- Interference—Pass or Fail. Indicates whether or not the interference level exceeds a threshold level.
- Coverage—Pass or Fail. Indicates whether or not the coverage level exceeds a threshold level.
- Controller Name—Name of the controller to which the access point is associated.
- Controller IP Address—IP address of the controller to which the access point is associated.

Figure 14-25 AP Profile Status Report Results



AP Profile Status

Generated: 2011-May-18, 09:00:14 UTC

Report By: AP By Controller

Protocol: 802.11a/n

Reporting Period: Last 1 day

Cisco Prime
Network Control System

AP Profile Status

Time	AP Name	Base Radio MAC	Radio Type	Load	Noise	Map Location	Controller Name
2011-May-18, 08:45:17 UTC	Pole9	00:0b:85:62:34:50	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	Pole19	00:0b:85:67:72:d0	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	Pole15	00:0b:85:6e:02:a0	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	Pole3_f	00:0b:85:6e:31:30	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	Roof12	00:0b:85:6e:e5:00	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	Pole14-lott	00:0b:85:6e:e6:80	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	Pole11_c2	00:0b:85:70:50:a0	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated
2011-May-18, 08:45:17 UTC	sjc5-r1awc-5150	00:0b:85:70:51:50	802.11a	Pass	Pass	Root Area	Not Associated
2011-May-18, 08:45:17 UTC	Pole14_c1	00:0b:85:70:6a:b0	802.11a	Pass	Pass	SkyCaptain > SiteFour	Not Associated

251875

Busiest APs

This report displays the access points with the highest total usage (transmitting, receiving, and channel utilization) on your wireless network.

Click **Busiest APs** from the Report Launch Pad to open the Busiest APs Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Busiest APs Reports page. See the "Configuring a Busiest APs Report" section on page 14-95 and the "Configuring a Busiest APs Report" section on page 14-95 for more information.

Configuring a Busiest APs Report

This section describes how to configure a Busiest APs report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Protocol—Choose **802.11 a/n** or **802.11 b/g/n** from the drop-down list.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Busiest APs report results include the following:

- AP Name—The access point name.
- Radio Type
- Rx Utilization (%)—The percentage of time that the access point receiver is busy operating on packets. The percentage (0 to 100%) represents a load from 0 to 1.
- Tx Utilization (%)—The percentage of time that the access point transmitter is busy operating on packets. The percentage (0 to 100%) represents a load from 0 to 1.
- Channel Utilization (%)—The percentage of time that an access point channel is busy operating on packets. The percentage (0 to 100%) represents a load from 0 to 1.
- Controller Name
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- Controller IP Address
- Client Count—The count of the access points that have the highest usage.

Busiest APs Report Results

The following are potential results for a Busiest APs report, depending on how the report is customized (see Figure 14-26):

- AP Name (mandatory column)
- Radio Type—802.11a/n or 802.11b/g/n.
- Rx Utilization (%)—The percentage of time the access point receiver is busy operating on packets. It is a number from 0-100 representing a load from 0 to 1.

- Tx Utilization (%)—This is the percentage of time the access point transmitter is busy operating on packets. It is a number from 0-100 representing a load from 0 to 1.
- Channel Utilization (%)—This is the percentage of time an access point channel is busy operating on packets. It is a number from 0-100 representing a load from 0 to 1.
- Controller Name and IP Address
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.

Figure 14-26 Busiest APs Report Results

Busiest APs

Generated: 2011-May-18, 09:15:32 UTC

Report By: AP By Controller

Protocol: 802.11a/n

Reporting Period: Last 7 days

Show: Up to 5 records

Cisco Prime
Network Control System

Busiest APs

AP Name	Radio Type	Rx Utilization (%)	Tx Utilization (%)	Channel Utilization (%)	Controller Name
kasi-evora	802.11a/n	0.03	0.13	45.69	Cisco_7d:88:00
hdelery-evora	802.11a/n	0	0	38	Cisco_7d:88:00
SJC14-21A-A13	802.11a/n	0.11	0.26	20.54	Cisco_d5:02:4f
SJC14-22A-AP-A16	802.11a	0	0	20.51	Cisco_d5:02:4f
SJC14-22A-AP-A3	802.11a	2.38	2.81	19.59	Cisco_d5:02:4f

251876

CPU Utilization

This report displays CPU utilization switch usage on your network.

Click **CPU Utilization** from the Report Launch Pad to open the CPU Utilization Report page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the CPU Utilization Report page. See the "Configuring a CPU Utilization Report" section on page 14-97 for more information.

Configuring a CPU Utilization Report

This section describes how to configure a CPU Utilization report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report Type:
  - Switch CPU Utilization
  - Top Switch CPU Utilization

- Report By:
  - Switch IP
  - Device Name
- Report Criteria—Choose **All Switches**, or click **Edit** to choose specific devices.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Choose a time period from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Detailed Switch Inventory

This report displays inventory information about the switches in your network.

Click **Detailed Switch Inventory** from the Report Launch Pad to open the Detailed Switch Inventory page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Detailed Switch Inventory page. See the "Configuring a Detailed Switch Inventory Report" section on page 14-98 for more information.

Configuring a Detailed Switch Inventory Report

This section describes how to configure a Detailed Switch Inventory report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By:
  - Device IP
  - Device Name
- Report Criteria—Choose **All Switches**, or click **Edit** to choose specific devices.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

The Detailed Switch Inventory report results include the following:

- Name
- Description
- Device IP Address
- Contact
- Location
- Sys Up Time

Identity Capability

This report displays the identity capability summary for the switches in your network.

Click **Identity Capability** from the Report Launch Pad to open the Identity Capability Report page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Identity Capability Report page. See the "Configuring an Identity Capability Report" section on page 14-99 for more information.

Configuring an Identity Capability Report

This section describes how to configure a Identity Capability report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Memory Utilization

This report displays the memory utilization summary for the switches in your network.

Click **Memory Utilization** from the Report Launch Pad to open the report page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Memory Utilization Report page. See the "Configuring a Memory Utilization Report" section on page 14-100 for more information.

Configuring a Memory Utilization Report

This section describes how to configure a Memory Utilization report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report Type:
  - Switch Memory Utilization
  - Top Switch Memory Utilization
- Report By:
  - Switch IP
  - Device Name
- Report Criteria—Choose **All Switches**, or click **Edit** to choose specific devices.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Choose a time period from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Non-Primary Controller APs

This report displays the access points that are not connected to the configured primary controller.

Click **Non-Primary Controller APs** from the Report Launch Pad to open the report page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Switch Interface Utilization page. See the "Configuring a Switch Interface Utilization Report" section on page 14-102 for more information.

Configuring a Non-Primary Controller APs Report

This section describes how to configure a Non-Primary Controller APs report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by—Choose **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to choose specific devices).

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Show—Enter the number of records that you want displayed in the report.

  Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

- Reporting Period
  - Choose a time period from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Non-Primary Controller APs Report Results

The following are potential results for a Non-Primary Controller APs report, depending on how the report is customized:

- AP Name—The name of the access point
- Base Radio MAC—The MAC address of the base radio.
- Map Location—The location of the access point in the map.
- Associated Controller Name—The name of the controller to which the access point is associated with.
- Primary Controller Name—The name of the primary controller to which the access point is associated with.

Switch Interface Utilization

This report displays the devices with the highest utilization on your network.

Click **Switch Interface Utilization** from the Report Launch Pad to open the report page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Switch Interface Utilization page. See the "Configuring a Switch Interface Utilization Report" section on page 14-102 for more information.

Configuring a Switch Interface Utilization Report

This section describes how to configure a Switch Interface Utilization report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report Type:
  - Top-N Rx Utilization
  - Top-N Tx Utilization
  - Bottom-N Rx Utilization
  - Bottom-N Tx Utilization

- Report By:
  - Device IP
  - Device Name
- Report Criteria—Choose **All Switches** or click **Edit** to choose specific devices.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Choose a time period from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

The Detailed Switch Inventory report results include the following:

- Device Name
- Device IP Address
- Interface Name
- Min Rx (%)
- Max Rx (%)
- Avg Rx (%)

Switch Interface Utilization Report Results

The following are potential results for a Switch Interface Utilization report, depending on how the report is customized:

- Device Name
- Device IP Address
- Interface Name
- Min Rx(%)
- Max Rx(%)
- Avg Rx(%)

AP Summary

This report displays a list of access points which are broadcasting SSID(s). This report allows you to filter the devices by RF group name, mobility group name, access point group name, SSID, location, and other statistics.

Note

- This report, by default, displays a list of access points that are broadcasting one or more SSIDs; the **All SSIDs** filter is chosen by default. Access points that are broadcasting no SSID are not displayed.
- The AP Summary report does not include Autonomous access points. For Autonomous access points, you need to run an Autonomous AP Summary report.

Click **AP Summary** from the Report Launch Pad to open the AP Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click New from the Report Launch Pad or from the AP Summary Reports page. See the "Configuring an AP Summary Report" section on page 14-104 and the "AP Summary Report Results" section on page 14-106 for more information.

Configuring an AP Summary Report

This section describes how to configure an AP Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - Floor Area—Choose **All Campuses > All Builders > All Floors** from the Report Criteria page, or click **Edit** to choose specific locations.
  - Outdoor Area—Choose **All Campuses > All Outdoor Areas** from the Report Criteria page, or click **Edit** to choose specific locations.
  - OfficeExtend AP—Choose **Enable** from the Report Criteria page, or click **Edit** to choose **Enable** or **Disable**.
  - AP by Controller—Choose **All Controllers > All APs** from the Report Criteria page, or click **Edit** to choose specific devices.

- AP Group—Choose **All AP Groups** from the Report Criteria page, or click **Edit** to choose a specific access point group.
- RF Group—Choose **All RF Groups** from the Report Criteria page, or click **Edit** to choose a specific radio frequency group.
- AP Mode—Choose **All AP Modes** from the Report Criteria page, or click **Edit** to choose a specific access point mode.

Note This report only returns monitor mode access points if **Report by AP Mode** is selected. Reports run by any other **Report by** selection drop all monitor mode access points from the results.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- SSID—Choose the appropriate SSID from the list. You can choose *None* to show all access points with no SSIDs configured.

Note The SSID filter is tied to all the criteria in the Report By category. This limits the scope for getting a report of access points by any scope listed in the Report By criteria. For this report to be able to retrieve access points by any Report By criteria, the default selection of All SSIDs should be used.

Note Access points must be broadcasting SSID(s) to satisfy the "All SSID" default filter of the report.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

AP Summary report results include the following:

- AP Name—The access point name.
- Ethernet MAC Address
- Base radio MAC Address
- Model

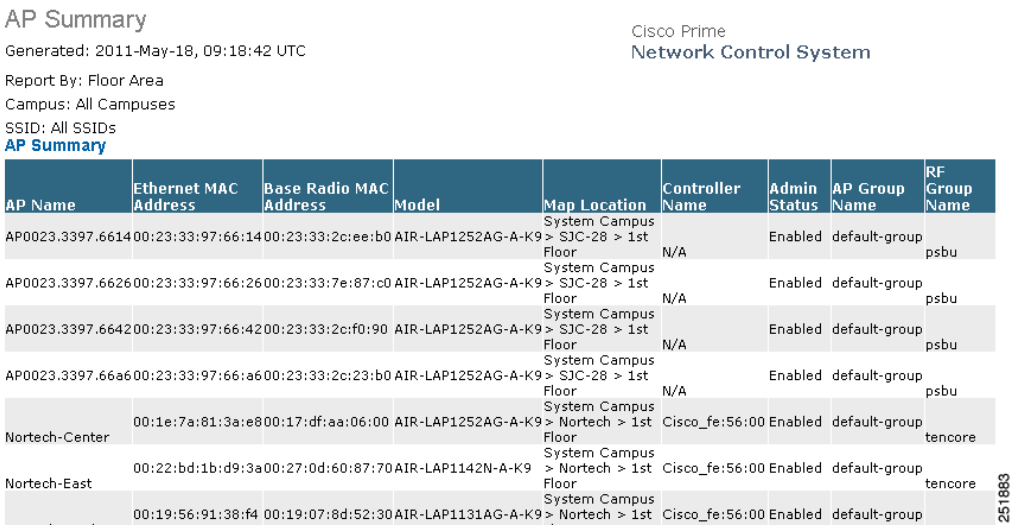
- Location
- Primary Controller
- Admin Status—Enable/Disable.
- AP group Name
- RF group Name
- Software Version
- Controller Version
- AP Mode—Local, Bridge, Rogue Detector, or FlexConnect.
- Associated WLANs—Associated SSIDs.
- 802.11a/n and 802.11b/g/n Status—Up/Down.
- Serial Number
- AP Type—Indicates the type of access point (unified or autonomous).

AP Summary Report Results

The following are potential results for an AP Summary report, depending on how the report is customized (see Figure 14-27):

- AP Name (mandatory column)
- Ethernet MAC Address
- Base Radio MAC Address
- Model
- Location
- Primary Controller
- Admin Status—Enabled or disabled.
- AP Group Name
- RF Group Name
- Software Version
- Controller Name
- AP Mode—Access point mode including: Local, Bridge, Rogue Detector, or FlexConnect.
- Associated WLANs—Associated SSIDs.
- 802.11a/n and 802.11b/g/n Status—Up or down.
- Serial Number

Figure 14-27 AP Summary Report Results



AP Summary

Generated: 2011-May-18, 09:18:42 UTC

Report By: Floor Area

Campus: All Campuses

SSID: All SSIDs

Cisco Prime
Network Control System

AP Summary

AP Name	Ethernet MAC Address	Base Radio MAC Address	Model	Map Location	Controller Name	Admin Status	AP Group Name	RF Group Name
AP0023.3397.6614	00:23:33:97:66:14	00:23:33:2c:ee:b0	AIR-LAP1252AG-A-K9	System Campus > SJC-28 > 1st Floor	N/A	Enabled	default-group	psbu
AP0023.3397.6626	00:23:33:97:66:26	00:23:33:7e:87:c0	AIR-LAP1252AG-A-K9	System Campus > SJC-28 > 1st Floor	N/A	Enabled	default-group	psbu
AP0023.3397.6642	00:23:33:97:66:42	00:23:33:2c:f0:90	AIR-LAP1252AG-A-K9	System Campus > SJC-28 > 1st Floor	N/A	Enabled	default-group	psbu
AP0023.3397.66a6	00:23:33:97:66:a6	00:23:33:2c:23:b0	AIR-LAP1252AG-A-K9	System Campus > SJC-28 > 1st Floor	N/A	Enabled	default-group	psbu
Nortech-Center	00:1e:7a:81:3a:e8	00:17:df:aa:06:00	AIR-LAP1252AG-A-K9	System Campus > Nortech > 1st Floor	Cisco_fe:56:00	Enabled	default-group	tencore
Nortech-East	00:22:bd:1b:d9:3a	00:27:0d:60:87:70	AIR-LAP1142N-A-K9	System Campus > Nortech > 1st Floor	Cisco_fe:56:00	Enabled	default-group	tencore
	00:19:56:91:38:f4	00:19:07:8d:52:30	AIR-LAP1131AG-A-K9	System Campus > Nortech > 1st	Cisco_fe:56:00	Enabled	default-group	

251883

Inventory

This report allows you to generate inventory-related information for controllers, access points, and MSEs managed by the NCS. This information includes hardware type and distribution, software distribution, CDP information, and other statistics.

Click **Inventory** from the Report Launch Pad to open the Inventory Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Inventory Reports page. See the "Configuring an Inventory Report" section on page 14-107 and the "Inventory Report Results" section on page 14-111 for more information.

Note The disassociated access points with model and serial number as **null** or **''** values are filtered out from the AP Inventory reports.

Configuring an Inventory Report

This section describes how to configure an Inventory report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report Type—Choose **Combined Inventory**, **APs**, **Autonomous APs**, **Controllers**, or **MSEs** from the drop-down list.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Note An Inventory report contains the following sections: Count of Controllers by Model, Count of Controllers by Software Version, Controller Inventory, Disassociated AP(s), Count of APs by Model, Count of APs by Software Version.
To customize report results for a particular section, choose the appropriate section from the Customizable Report drop-down list.

Count of Controllers by Model results contain the following information:

- Model Name—The name of the model of the controller.
- Number of Controllers—The controller count for each model name.

Available information for Count of Controllers by Model results contain the following:

- Software Version—The software version of the controller.
- Number of Controllers—The controller count for each software version.

Controller Inventory results contain the following information:

- Controller Name
- IP Address—The IP address of the controller.
- Location—The user-specified physical location of the controller.
- Interfaces—The names of the interfaces of the controller combined together by commas.
- Reachability Status—*Reachable* if the controller is currently manageable.
- Serial Number—The serial number of the controller.
- Model—The model name of the controller.
- Software Version—The software version of the controller.
- Mobility Group—The name of the mobility group to which the controller is assigned.
- RF Group—The name of the RF group to which the controller is assigned.
- Neighbor Name, Port, and Address—CDP neighbor information including the name, port, and IP address of the neighbor.
- Duplex—The duplex mode of the CDP neighbor interface.

Count of APs by Model results contain the following information:

- Model Name—The name of the model of the access point.
- Number of APs—The access point count for each model name.

Count of APs by Software Version results contain the following information:

- Software Version—The software version of the access point.
- Number of APs—The access point count for each software version.

AP Inventory results contain the following information:

- AP Name—The access point name.
- Ethernet MAC Address—The Ethernet MAC address of the access point.
- IP Address—The IP address of the access point.
- Model—The name of the model of the access point.
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- Controller Name—The name of the controller to which the access point is associated.
- Base radio MAC Address—The MAC address of an access point.
- Software Version—The software version of an access point.
- Location—The user-specified physical location of an access point.
- Primary Controller—The name of the primary controller to which the access point should associate. When the access point is not directly connected to a controller, it tries to find the primary controller and associates with it. If this attribute is empty or an access point is unable to find the controller with this name, it associates with the secondary controller.
- Secondary Controller—The name of the secondary controller to which the access point should associate if the primary controller is unavailable. If the primary and secondary controllers are not available, the access point associates with the tertiary controller.
- Tertiary Controller—The name of the tertiary controller to which the access point should associate if the primary and secondary controller is unavailable. If the primary, secondary, and tertiary switch are unavailable, it associates with the master controller.
- Admin Status—The admin status of the access point.
- AP Mode—The monitor only mode setting of the access point. The options are local, monitor, FlexConnect, rogue detector, sniffer, and bridge.
- 802.11 a/n and 802.11 b/g/n Status—The operation state of the respective radio. The options are down, up, not associated, and unknown.
- Gateway—The gateway for the access point.
- Netmask—The netmask of the IP address of the access points.
- IOS and Boot Versions—The version of the IOS Cisco access point, and the major/minor boot version of the access point.
- Certificate Type—The access point certification type options are unknown, manufacture installed, self signed, or local significance.
- Serial Number—The serial number of the access point.
- Neighbor Name, Address, Port, and Advertised Version—The CDP neighbor name, IP address, port, and advertised version information of the access point.

Disassociated AP(s) results contain the following information:

- AP Name—The access point name.
- Ethernet MAC Address—The Ethernet MAC address of the access point.

- IP Address—The IP address of the access point.
- Model—The name of the model of the access point.
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- Controller Name—The name of the controller to which the access point is associated.
- Base radio MAC Address—The MAC address of an access point.
- Software Version—The software version of an access point.
- Location—The user-specified physical location of an access point.
- Primary Controller—The name of the primary controller to which the access point should associate. When the access point is not directly connected to a controller, it tries to find the primary controller and associates with it. If this attribute is empty or an access point is unable to find the controller with this name, it associates with the secondary controller.
- Secondary Controller—The name of the secondary controller to which the access point should associate if the primary controller is unavailable. If the primary and secondary controllers are not available, the access point associates with the tertiary controller.
- Tertiary Controller—The name of the tertiary controller to which the access point should associate if the primary and secondary controller is unavailable. If the primary, secondary, and tertiary switch are unavailable, it associates with the master controller.
- Admin Status—The admin status of the access point.
- AP Mode—The monitor only mode setting of the access point. The options are local, monitor, FlexConnect, rogue detector, sniffer, and bridge.
- 802.11 a/n and 802.11 b/g/n Status—The operation state of the respective radio. The options are down, up, not associated, and unknown.
- Gateway—The gateway for the access point.
- Netmask—The netmask of the IP address of the access point.
- IOS and Boot Versions—The version of the IOS Cisco access point, and the major/minor boot version of the access point.
- Certificate Type—The access point certification type options are unknown, manufacture installed, self signed, or local significance.
- Serial Number—The serial number of the access point.
- Neighbor Name, Address, and Port—The CDP neighbor name, IP address, and port information of the access point.
- Duplex—CDP Neighbor interface duplex mode.
- AP Type—Indicates the type of access point (unified or autonomous).

Note The AP Inventory report displays only associated access points in the network.

Note The disassociated access points with model and serial number as *null* or '' values are filtered out from the AP Inventory reports.

Count of MSEs by Version results contain the following information:

- Version—The MSE version.
- Number of MSEs—The count of both MSE and Location Servers.

MSEs results contain the following information:

- Device Name—The name of the MSE or Location Server.
- IP Address
- Device Type
- HTTP/HTTPS Port
- HTTPS
- Version
- Start Time

Inventory Report Results

The following are potential results for an Inventory report, depending on how the report is customized (see Figure 14-28):

- Count of Controllers by Model results
  - Model Name (mandatory column)—Name of the model of the controller.
  - Number of Controllers (mandatory column)—Controller count for each model name.
- Count of Controllers by Model results
  - Software Version (mandatory column)—Software version of the controller.
  - Number of Controllers (mandatory column)—Controller count for each software version.
- Controller Inventory results
  - Controller Name (mandatory column)
  - IP Address—IP address of the controller.
  - Location—User specified physical location of the controller.
  - Interfaces—The names of the interfaces of the controller combined together by commas.
  - Reachability Status—Reachable if the controller is currently manageable.
  - Serial Number—Serial number of the controller.
  - Model—Model name of the controller.
  - Software Version—Software version of the controller.
  - Mobility Group—The name of the mobility group to which the controller is assigned.
  - RF Group—The name of the RF group to which the controller is assigned.
  - Neighbor Name, Port, and Address—CDP Neighbor information including the name, port and IP address of the neighbor.
  - Duplex—CDP Neighbor interface duplex mode.
- Count of APs by Model results
  - Model Name (mandatory column)—Name of the model of the access point.
  - Number of APs (mandatory column)—Access point count for each model name.
- Count of APs by Software Version results

  - Software Version (mandatory column)—Software version of the access point.
  - Number of APs (mandatory column)—Access point count for each software version.
- AP Inventory results
  - AP Name (mandatory column)
  - Ethernet MAC Address—Ethernet MAC address of the access point.
  - IP Address—IP address of the access point.
  - Model—Name of the model of the access point.
  - Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
  - Controller Name—Name of the controller to which the access point is associated.
  - Base Radio MAC Address—The MAC address of an access point base radio.
  - Software Version—The software version of an access point.
  - Location—User specified physical location of the access point.
  - Primary Controller—Name of the controller identified as the primary controller of the access point with which the access point should associate. When the access point is not directly connected to a controller, it tries to find the primary controller and associates with it. If this attribute is empty or if the access point is not able to find the controller with this name, then it associates with the secondary controller.
  - Secondary Controller—Name of the controller identified as the secondary controller of the access point with which access point should associate if the primary controller is not available.

    If primary and secondary controllers are not available, then the access point associates with the tertiary controller.
  - Tertiary Controllers—Name of the controller identified as the tertiary controller of the access point with which access point should associate if the primary or secondary controllers are not available.

    If primary, secondary and tertiary switch are not available, then it associates with the master controller.
  - Admin Status—Administrative state of the access point.
  - AP Mode—Mode setting of the access point. Possible modes include: Local, Monitor, FlexConnect, Rogue Detector, Sniffer, and Bridge.
  - 802.11 a/n and 802.11 b/g/n Status—Operation state of the respective radio. Possible statuses include Down, Up, Not Associated, and Unknown.
  - Gateway—The gateway for the access point.
  - Netmask—The netmask of the access point IP address.
  - IOS Version—Version of the Cisco IOS access point.
  - Boot Version—Major and Minor boot version of the access point.
  - Certificate Type—Access point certification type. Possible types include: Unknown, Manufacture Installed, Self Signed, and Local Significance.
  - Serial Number—Serial number of the access point.
  - Neighbor Name, Address, Port, and Advertised Version—The access point CDP neighbor name, IP address, port, and advertised version information.
- Inventory results

- AP Name (mandatory column)
- Ethernet MAC Address
- IP Address
- Model
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- 802.11 a/n and 802.11 b/g/n MAC Addresses
- Software Version
- Location
- Reachability Status
- 802.11 a/n and 802.11 b/g/n Status
- Serial Number

Figure 14-28 Inventory Report Results

Inventory Report

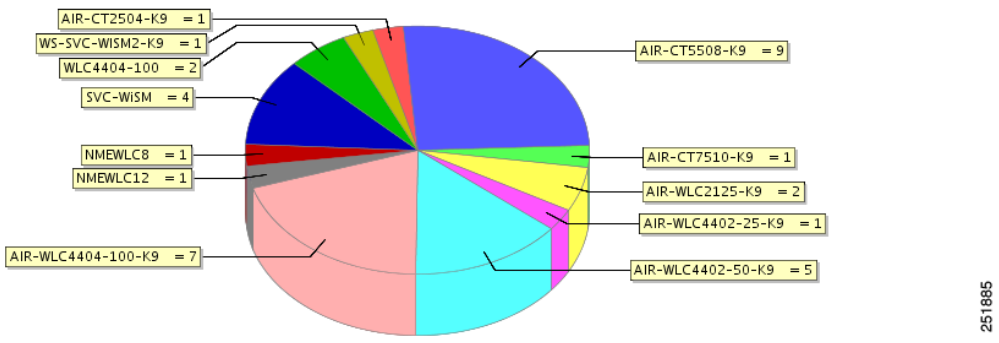
Generated: 2011-May-18, 09:21:10 UTC

Cisco Prime
Network Control System

Count of Controllers by Model

Model Name	Number of Controllers
AIR-CT2504-K9	1
AIR-CT5508-K9	9
AIR-CT7510-K9	1
AIR-WLC2125-K9	2
AIR-WLC4402-25-K9	1
AIR-WLC4402-50-K9	5
AIR-WLC4404-100-K9	7
NMEWLC12	1
NMEWLC8	1
SVC-WiSM	4
WLC4404-100	2
WS-SVC-WISM2-K9	1

Controllers by Model



Uptime

This report displays the access point uptime, the LWAPP uptime, and the LWAPP join time.

Click **Uptime** from the Report Launch Pad to open the Uptime Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Uptime Reports page. See the "Configuring an Uptime Report" section on page 14-114 and the "Configuring an Uptime Report" section on page 14-114 for more information.

Configuring an Uptime Report

This section describes how to configure an AP Image Predownload report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Uptime report results contain the following information:

- AP Name—The access point name.
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- AP Uptime—The time duration since the last access point reboot.
- LWAPP Uptime—The time duration since the last access point joined the controller.
- LWAPP Join Taken Time—The time it took for the access point to join the controller. This value could be significant in Mesh environments.

Uptime Report Results

The following are potential results for an Uptime report, depending on how the report is customized (see Figure 14-29):

- AP Name
- Map Location—The building, floor area, or outdoor area (as applicable) where the access point is located.
- AP Uptime—The length of time since the access point last rebooted.
- LWAPP Uptime—The length of time since the access point last joined the controller.
- LWAPP Join Taken Time—The amount of time the access point took to join the controller.

Note This could be a significant value in mesh environments.

Figure 14-29 Uptime Report Results

Up Time

Generated: 2011-May-18, 09:25:29 UTC

Report By: AP By Controller

Show: Up to 10 records

Cisco Prime
Network Control System

Up Time

AP Name	Controller Name	Map Location	AP Up Time
z-khi-1142-c	Cisco_7d:88:00	System Campus > Home-AP > 11	22 mins 22 secs
rraghuna-homeap	Cisco_fe:54:20		34 mins 36 secs
ykondare-homeap	Cisco_fe:54:20		2 hrs 45 mins 49 secs
sumnguye-homeap	oeap-talwar-2		3 hrs 3 mins 5 secs
shpoon-homeap	oeap-talwar-2		3 hrs 24 mins 14 secs
law-homeap	oeap-talwar-2	System Campus > Home-AP > 10	3 hrs 26 mins 26 secs
dstumbau-homeap	Cisco_fe:54:20	System Campus > Home-AP > 9	6 hrs 6 mins 52 secs
nsarwary-evora	Cisco_7d:88:00		6 hrs 16 mins 6 secs
jimorri2-homeap	Cisco_fe:54:20		6 hrs 46 mins 4 secs
rahutson-homeap	oeap-talwar-2	System Campus > Home-AP > 3rd floor	6 hrs 47 mins 44 secs

251904

Utilization

This report displays the controller, AP, and MSE usage on your wireless network. These statistics (such as CPU usage, memory usage, link utilization, and radio utilization) can help identify current network performance and help with capacity planning for future scalability needs.

Click **Utilization** from the Report Launch Pad to open the Utilization Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Utilization Reports page. See the "Configuring a Utilization Report" section on page 14-116 and the "Utilization Report Results" section on page 14-117 for more information.

Configuring a Utilization Report

This section describes how to configure a Utilization report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report Type—Choose **Controllers**, **MSEs**, or **Radios** from the drop-down list.
- Report by (Report by options change depending on the report type chosen)
  - Controller—If the report type is Controllers, choose **All Controllers** from the Report Criteria page, or click **Edit** to choose specific devices. Depending on the report type selected, you receive either radio or controller utilization results. See the "Radio, Controller, and MSE Utilization Results" section on page 14-116.
  - MSEs—If the report type is MSEs, choose **All MSEs** from the Report Criteria page, or click **Edit** to choose specific devices. Depending on the report type selected, you receive either radio or controller utilization results. See the "Radio, Controller, and MSE Utilization Results" section on page 14-116.
  - Radios—If the report type is Radio, choose **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to choose specific devices). Depending on the report type chosen, you receive either radio or controller utilization results. See the "Radio, Controller, and MSE Utilization Results" section on page 14-116.

Note In the Radios Report Criteria page, you can choose **All Access Points** or **All OfficeExtend Access Points**.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select **802.11 a/n**, **802.11 b/g/n**, or both. This field only appears if the report type is Radios.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Radio, Controller, and MSE Utilization Results

Depending on the report type chosen, you receive either radio, controller, or MSE utilization results.

- Radio Utilization

  - Rx Utilization (%)—The percentage of time that the access point receiver is busy operating on packets. The percentage (from 0 to 100%) represents a load from 0 to 1.
  - Tx Utilization (%)—The percentage of time the access point transmitter is busy operating on packets. The percentage (from 0 to 100%) represents a load from 0 to 1.
  - Channel Utilization (%)—The percentage of time an access point channel is busy operating on packets. The percentage (from 0 to 100%) represents a load from 0 to 1.
- Controller Utilization
  - CPU Utilization—The percentage of CPU utilization.
  - Memory Utilization—The percentage of memory utilization.
  - Port Utilization—The percentage of (totalDeltaBits/bandwidth) on a port.
- MSE Utilization
  - CPU Utilization—The percentage of CPU utilization.
  - Memory Utilization—The percentage of memory utilization.

Schedule

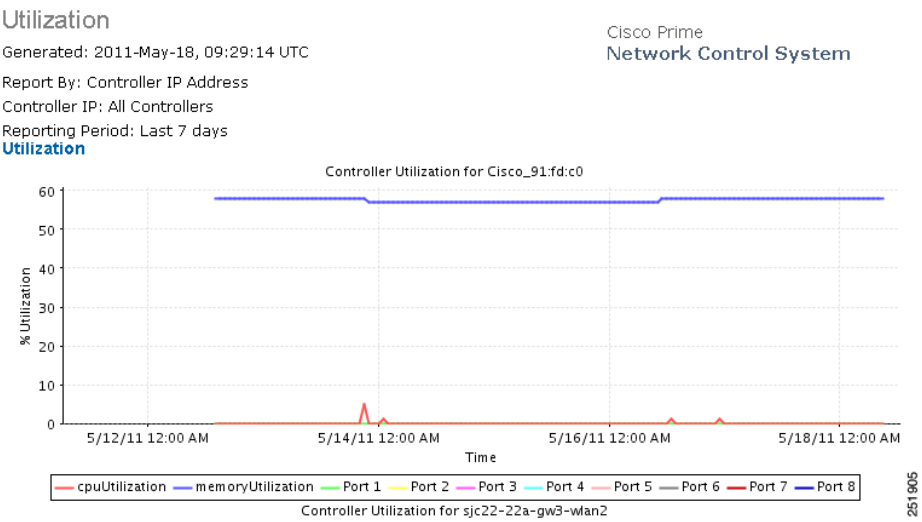
If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Utilization Report Results

The following are potential results for a Utilization report (see Figure 14-30):

- Controller results including CPU, memory, and port utilization.
  - CPU Utilization—The percentage of CPU utilization.
  - Memory Utilization—The percentage of memory utilization.
  - Port Utilization—The percentage of (totalDeltaBits/bandwidth) on a port.
- Radio results including channel, transmitting, and receiving utilization.
  - Channel Utilization—The percentage of time an AP channel is busy operating on packets. It is a number from 0-100 representing a load from 0 to 1.
  - Rx Utilization—The percentage of time the AP receiver is busy operating on packets. It is a number from 0-100 representing a load from 0 to 1.
  - Tx Utilization—The percentage of time the AP transmitter is busy operating on packets. It is a number from 0-100 representing a load from 0 to 1.
- MSE results including memory utilization, CPU utilization, Context Aware Service statistics.
  - MSE CPU Utilization—The percentage of CPU utilization.
  - MSE Memory Utilization—The percentage of memory utilization.
  - Context Aware Service Statistics—Provides a graph of the count of the number of Clients, Tags, Rogue Client, Rogue APs, and Adhoc Rogue APs over a period of time.

Figure 14-30 Utilization Report Results



MSAP Reports

This section describes the MSAP reports you can create and contains the following topics:

- Mobile MAC Statistics, page 14-118
- Service URI Statistics, page 14-119

Note For more information about adding and deleting MSAP, see the "MSAP" section on page 11-97.

Mobile MAC Statistics

Click **Mobile MAC Statistics** from the Report Launch Pad to open the Mobile MAC Statistics Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Mobile MAC Statistics Reports page, see the "Configuring a Mobile MAC Statistics Report" section on page 14-118 for more information.

Configuring a Mobile MAC Statistics Report

This section describes how to configure an Mobile MAC Statistics report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by

  - Mobile MAC by MSAP Server—Choose this option if you want to generate a report on mobile MACs based on MSAP servers.
  - Mobile MAC by Venue—Choose this option if you want to generate a report on mobile MACs based on venue.
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and choose the required filter criteria.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

The Mobile MAC Statistics report results contain the following:

- Mobile MAC
- Click Count

Note This report provides Most Active Mobile MACs based on click count by MSE and/or by Venue. If multiple MSEs are selected, top Mobile MACs are grouped by each MSE in the selected sorting order.

Service URI Statistics

Click **Service URI Statistics** from the Report Launch Pad to open the Service URI Statistics Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Mobile MAC Statistics Reports page, see the "Configuring a Service URI Statistics Report" section on page 14-120 for more information.

Configuring a Service URI Statistics Report

This section describes how to configure an Service URI Statistics report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - Service URI by MSAP Server—Choose this option if you want to generate a report on mobile MACs based on MSAP servers.
  - Service URI by Venue—Choose this option if you want to generate a report on the Service URIs based on Venue.
  - Service URI by Mobile MAC—Choose this option if you want to generate a report on the Service URIs based on Mobile MAC.
  - Service URI by Provider—Choose this option if you want to generate a report on the Service URIs based on Provider.
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and choose the required filter criteria.

  Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

The Service URI Statistics report results contain the following:

- Service URI
- Mobile MAC
- Click Count

Note This report provides Top Service URIs based on click count by MSE and/or by Venue. If the multiple MSEs are selected, top Service URIs are grouped by each MSE in the selected sorting order.

Guest Reports

This section describes the Guest reports you can create and contains the following topics:

Guest Accounts Status

This report displays guest account status changes in chronological order. The report filters guest accounts by the guest user who created them. One example of a status change is Scheduled to Active to Expired.

Click **Guest Accounts Status** from the Report Launch Pad to open the Guest Accounts Status Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Guest Accounts Status Reports page. See the "Configuring a Guest Accounts Status Report" section on page 14-121 for more information.

Configuring a Guest Accounts Status Report

This section describes how to configure an Accounts Status report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - NCS User—Choose **All NCS Users** from the Report Criteria page, or click **Edit** to choose a specific NCS user.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Guest Account Status report results contain the following information:

- Time
- Guest username
- Created by
- Status

Guest Account Status Report Results

The following are potential results for a Guest Account Status report, depending on how the report is customized:

- Time
- Guest Username
- Created by
- Status

Guest Association

This report displays when a guest client associated to and disassociated from a guest profile/SSID over a customizable period of time.

Click **Guest Association** from the Report Launch Pad to open the Guest Association Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Guest Association Reports page. See the "Configuring a Guest Association Report" section on page 14-123 for more information.

Configuring a Guest Association Report

This section describes how to configure a Guest Association report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - Guest Profile—Choose **All Profiles** from the Report Criteria page, or click **Edit** to choose a specific profile.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Guest Association report results contain the following information:

- Time
- Guest user
- Guest MAC address
- Controller IP Address
- Global Unique
- Local Unique
- Link Local
- AP MAC Address
- Login and Logout Times
- Guest IP address
- Bytes Received
- Bytes Sent

Guest Association Report Results

The following are potential results for a Guest Association report, depending on how the report is customized:

- Time
- Guest MAC address and username
- Device IP address
- Guest profile
- Status
- AP Name
- Guest IP address
- Session Duration
- Reason—Reason for the disassociation

Guest Count

This report displays the number of guest clients logged into the network per guest profile/SSID over a customizable period of time.

Click **Guest Count** from the Report Launch Pad to open the Guest Count Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Guest Count Reports page. See the "Configuring a Guest Count Report" section on page 14-125 and the "Guest Count Report Results" section on page 14-125 for more information.

Configuring a Guest Count Report

This section describes how to configure a Guest Count report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - Guest Profile—Choose **All Profiles** from the Report Criteria page, or click **Edit** to choose a specific profile.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Select **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Guest Count Report Results

The Guest Count results contain the following information:

- Authenticated Guest Count—Indicates the number of authenticated guests for each specified guest profile and protocol during the specified period of time.

Guest User Sessions

This report displays historic session data for a guest user. The session data such as amount of data passed, login and logout time, guest IP address, and guest MAC address is available for one month by default. The data retention period can be configured from the Administration > Background Tasks page. This report can be generated for guest users who are associated to controllers running software Version 5.2 or later.

Click **Guest User Sessions** from the Report Launch Pad to open the Guest User Sessions Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Guest User Sessions Reports page. See the "Configuring a Guest User Sessions Report" section on page 14-126 and the "Guest User Sessions Report Results" section on page 14-126 for more information.

Note You cannot upgrade the Guest User Sessions reports to the NCS Release 1.1.

Configuring a Guest User Sessions Report

This section describes how to configure a Guest User Sessions report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - Guest User—Choose **All Guest Users** from the Report Criteria page, or click **Edit** to choose a specific guest user.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

Schedule

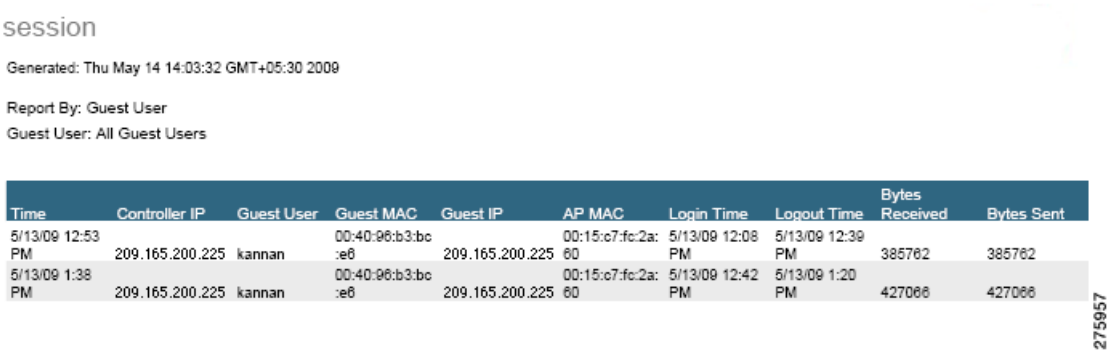
If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Guest User Sessions Report Results

The following are potential results for a Guest User Sessions report, depending on how the report is customized (see Figure 14-31):

- Time (mandatory column)
- Guest User (mandatory column)
- Guest User MAC Address (mandatory column)
- Controller IP Address
- Login Time
- Logout Time
- Guest IP Address
- Global Unique
- Local Unique
- Link Local
- Bytes Received
- Bytes Sent

Figure 14-31 Guest User Sessions Report Results



session

Generated: Thu May 14 14:03:32 GMT+05:30 2009

Report By: Guest User

Guest User: All Guest Users

Time	Controller IP	Guest User	Guest MAC	Guest IP	AP MAC	Login Time	Logout Time	Bytes Received	Bytes Sent
5/13/09 12:53 PM	209.165.200.225	kannan	00:40:96:b3:bc:e6	209.165.200.225	00:15:c7:fc:2a:60	5/13/09 12:08 PM	5/13/09 12:39 PM	385762	385762
5/13/09 1:38 PM	209.165.200.225	kannan	00:40:96:b3:bc:e6	209.165.200.225	00:15:c7:fc:2a:60	5/13/09 12:42 PM	5/13/09 1:20 PM	427066	427066

275957

NCS Guest Operations

This report displays all activities performed by one or all guests, such as creating, deleting, or updating guest user accounts. If a guest user is deleted from the NCS, the report still shows an activity performed by the deleted guest user for up to one week after the activity occurred.

Click **NCS Guest Operations** from the Report Launch Pad to open the NCS Guest Operations Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the NCS Guest Operations Reports page. See the "Configuring an NCS Guest Operations Report" section on page 14-127 and the "NCS Guest Operation Report Results" section on page 14-128 for more information.

Configuring an NCS Guest Operations Report

This section describes how to configure an NCS Guest Operations report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - NCS User—Choose **All NCS Users** from the Report Criteria page, or click **Edit** to choose a specific user.

Note All NCS Users consists of the Lobby ambassador user groups and those Users who have done at least one guest account operation.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.

– From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Guest Operation report results contain the following information:

- Time
- Reason
- NCS User
- Guest User
- Operation
- Status

NCS Guest Operation Report Results

The following are potential results for an NCS Guest Operations report, depending on how the report is customized:

- Time
- NCS User
- Guest User
- Operation
- Status
- Reason

Identity Services Engine Reports

Cisco ISE 1.0 is a consolidated policy-based access control system that is integrated into the NCS 1.0. ISE helps in the monitoring of endpoint security policy to deliver visibility into compliance based on real-time contextual information from the network, users, and devices across the entire wired and wireless access network.

The following Identity Services Engine reports could be generated using the NCS Report Launch pad:

- Posture Detail Assessment
- Endpoint Profiler Summary
- Top N Endpoint MAC Authentications
- Endpoint MAC Authentication Summary
- User Authentication Summary
- Top N User Authentications
- Radius Accounting
- Radius Authentication

Note

- You can view the ISE reports in the Report Launch pad only when an ISE is added to the NCS.
- To run the ISE reports, you need to enable the Identity Search Engine permission flag in the NCS > Administration > AAA > Groups > Group Detail menu option for the Super User, Config User, Admin, and System Monitoring user groups.
- When you launch the ISE reports from the NCS using Internet Explorer 8, the report does not appear properly. To view the report properly, refresh the content area (not the browser) by right clicking the report details and selecting the **Refresh this frame** option.

For more information on these reports, see the Available Reports section of the Reporting chapter of the *Cisco Identity Services Engine User Guide, Release 1.0*:
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

Mesh Reports

This section describes the Mesh reports and contains the following topics:

Alternate Parent

This report displays the number of alternate parents with the same configured mesh group for each mesh access point. This report can be used to determine an access point capability to handle failures in the mesh path.

Click **Alternate Parent** from the Report Launch Pad to open the Alternate Parent Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Alternate Parent Reports page. See the "Configuring an Alternate Parent Report" section on page 14-130 and the "Alternate Parent Report Results" section on page 14-130 for more information.

Configuring an Alternate Parent Report

This section describes how to configure an Alternate Parent report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Alternate Parent report results contain the following information:

- AP Name—The access point name.
- MAC address
- Parent AP name
- Number Alternate parents
- Parent MAC address

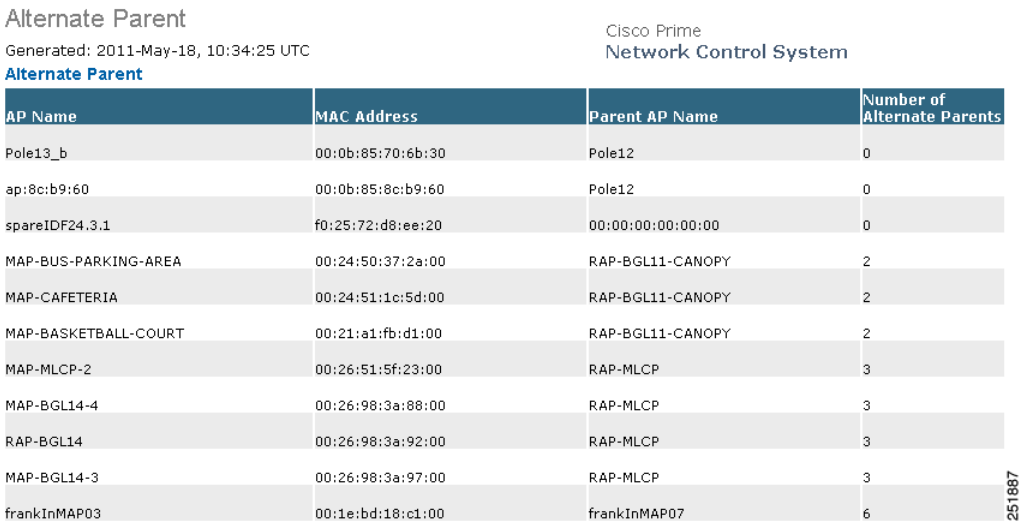
Alternate Parent Report Results

The following are potential results for an Alternate Parent report, depending on how the report is customized (see Figure 14-32):

- AP Name (mandatory column)
- MAC Address—The MAC address of the alternate parent.

- Parent AP Name and MAC Address
- Number of Alternate Parents

Figure 14-32 Alternate Parent Report Results



Alternate Parent

Generated: 2011-May-18, 10:34:25 UTC

Cisco Prime
Network Control System

Alternate Parent

AP Name	MAC Address	Parent AP Name	Number of Alternate Parents
Pole13_b	00:0b:85:70:6b:30	Pole12	0
ap:8c:b9:60	00:0b:85:8c:b9:60	Pole12	0
spareIDF24.3.1	f0:25:72:d8:ee:20	00:00:00:00:00:00	0
MAP-BUS-PARKING-AREA	00:24:50:37:2a:00	RAP-BGL11-CANOPY	2
MAP-CAFETERIA	00:24:51:1c:5d:00	RAP-BGL11-CANOPY	2
MAP-BASKETBALL-COURT	00:21:a1:fb:d1:00	RAP-BGL11-CANOPY	2
MAP-MLCP-2	00:26:51:5f:23:00	RAP-MLCP	3
MAP-BGL14-4	00:26:98:3a:88:00	RAP-MLCP	3
RAP-BGL14	00:26:98:3a:92:00	RAP-MLCP	3
MAP-BGL14-3	00:26:98:3a:97:00	RAP-MLCP	3
frankInMAP03	00:1e:bd:18:c1:00	frankInMAP07	6

251887

Link Stats

This report displays mesh link and node statistics such as parent access point, link SNR, packet error rate, parent changes, node hops, total transmit packets, mesh path, connected access points, mesh group, data rate, and channel. The mesh link and mesh node statistics can be run individually or combined.

Click **Link Stats** from the Report Launch Pad to open the Link Stats Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Link Stats Reports page. See the "Configuring a Link Stats Report" section on page 14-131 and the "Link Stats Report Results" section on page 14-132 for more information.

Configuring a Link Stats Report

This section describes how to configure a Link Stats report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report Type—Choose **Link Stats** or **Node Hops** from the drop-down list.
- Report by—Choose **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to choose specific devices).

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Link Stats report results contain the following information:

- Time
- MAC address
- Parent MAC address
- AP Name—The access point name.
- Parent AP name
- Link SNR
- Packet Error Rate
- Parent changes
- Parent changes per minute
- Node hops
- Total Tx Packets
- Total Tx Packets per minute

Link Stats Report Results

The following are potential results for a Link Stats report, depending on how the report is customized (see Figure 14-33):

- Time (mandatory column)
- MAC Address (mandatory column)
- Parent MAC Address (mandatory column)
- AP Name
- Parent AP Name
- Link SNR
- Packet Error Rate—Packet error rate percentage = 1- (number of successfully transmitted packets/number of total packets transmitted)
- Parent Changes and Parent Changes per Minute
- Node hops—The number of hops between access points
- Total Tx Packets and Total Tx Packets per Minute

Figure 14-33 Link Stats Report Results

Link Stats

Generated: 2011-May-18, 16:54:25 UTC

Report By: AP By Controller

Reporting Period: Last 3 days

Cisco Prime
Network Control System

Link Stats

Time	MAC Address	Parent MAC Address	AP Name	Parent AP Name	Link SNR	Packet Error Rate
2011-May-15, 16:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	26	0.04
2011-May-15, 17:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	25	0.04
2011-May-15, 18:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	25	0.04
2011-May-15, 19:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	24	0.04
2011-May-15, 20:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	25	0.04
2011-May-15, 21:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	25	0.04
2011-May-15, 22:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	26	0.04
2011-May-15, 23:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	25	0.04
2011-May-16, 00:59:59 UTC	58:bc:27:c4:23:00	58:bc:27:8b:e9:00	frankInMAP05	FrankenRAP01	26	0.04

251886

Nodes

This report displays mesh tree information for each mesh access point such as hop count, number of directly connected children, number of connected access points, and mesh path.

Click **Nodes** from the Report Launch Pad to open the Mesh Nodes Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Mesh Nodes Reports page. See the "Configuring a Nodes Report" section on page 14-133 and the "Configuring a Nodes Report" section on page 14-133 for more information.

Configuring a Nodes Report

This section describes how to configure a Nodes report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Format allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Node report results contain the following information:

- MAC Address—The MAC address of the mesh access point.
- AP Name—The name of the mesh access point.
- Node Hops—The number of node hops for this mesh group.
- Children—The number of children for this access point.
- Connected APs—The number of access points connected to this access point.
- Mesh Path—The path of the mesh access point.
- Controller—The controller to which the mesh access point is associated.
- Mesh Role—Mesh access point (MAP) or Root access point (RAP).
- Mesh Group—The name of the mesh group to which this access point belongs.
- Data Rate—The data rate for this access point.
- Channel—The channel on which this access point is located.

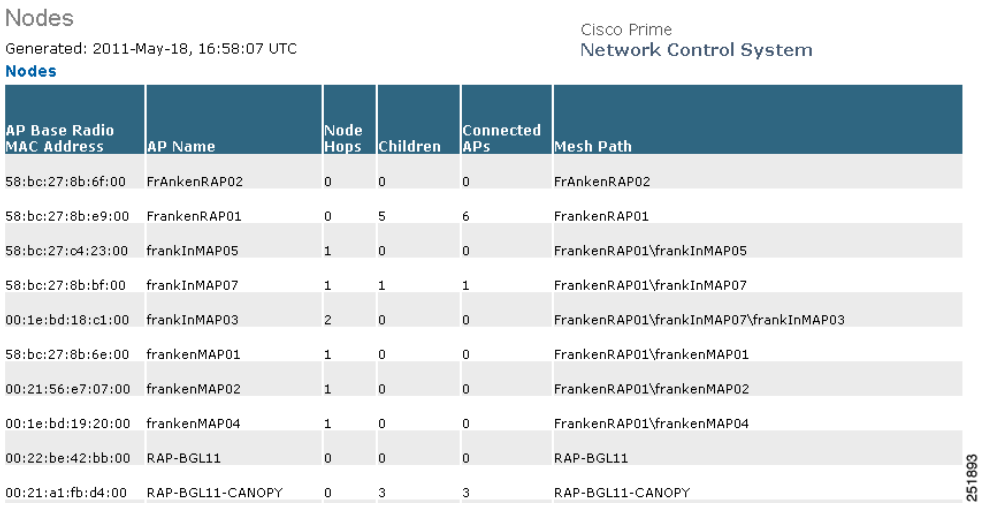
Nodes Report Results

The following are potential results for a Nodes report, depending on how the report is customized (see Figure 14-34):

- AP Name (mandatory column).
- AP MAC Address (mandatory column).
- Node Hops—The number of hops between access points.
- Children—The number of children for this access point.
- Connected APs—The number of access points connected to this access point.
- Mesh Path—The path of the mesh access point.
- Controller—The controller to which the mesh access point is associated.
- Mesh Role—Mesh access point (MAP) or Root access point (RAP).
- Mesh Group—The name of the mesh group to which this access point belongs.

- Data Rate—The data rate for this access point.
- Channel—The channel on which this access point is located.

Figure 14-34 Node Report Results



Nodes

Generated: 2011-May-18, 16:58:07 UTC

Cisco Prime
Network Control System

Nodes

AP Base Radio MAC Address	AP Name	Node Hops	Children	Connected APs	Mesh Path
58:bc:27:8b:6f:00	FrAnkenRAP02	0	0	0	FrAnkenRAP02
58:bc:27:8b:e9:00	FrankenRAP01	0	5	6	FrankenRAP01
58:bc:27:c4:23:00	frankInMAP05	1	0	0	FrankenRAP01\frankInMAP05
58:bc:27:8b:bf:00	frankInMAP07	1	1	1	FrankenRAP01\frankInMAP07
00:1e:bd:18:c1:00	frankInMAP03	2	0	0	FrankenRAP01\frankInMAP07\frankInMAP03
58:bc:27:8b:6e:00	frankenMAP01	1	0	0	FrankenRAP01\frankenMAP01
00:21:56:e7:07:00	frankenMAP02	1	0	0	FrankenRAP01\frankenMAP02
00:1e:bd:19:20:00	frankenMAP04	1	0	0	FrankenRAP01\frankenMAP04
00:22:be:42:bb:00	RAP-BGL11	0	0	0	RAP-BGL11
00:21:a1:fb:d4:00	RAP-BGL11-CANOPY	0	3	3	RAP-BGL11-CANOPY

251893

Packet Stats

This report displays the total number of packets transmitted, packets transmitted per minute, packet queue average, packet dropped count, packets dropped per minute, and errors for packets transmitted by neighbor access points. A report type can be chosen for each data type.

Click **Packet Stats** from the Report Launch Pad to open the Packet Stats Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Packet Stats Reports page. See the "Configuring a Packet Stats Report" section on page 14-135 and the "Packet Stats Report Results" section on page 14-136 for more information.

Configuring a Packet Stats Report

This section describes how to configure a Packet Stats report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report Type—Choose **Packet Stats** from the drop-down list.
- Report by—Choose **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to choose specific devices).

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Graph Type—Choose the type of graph you want displayed for these report results (Packet Counts or Packets Per Minute).
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

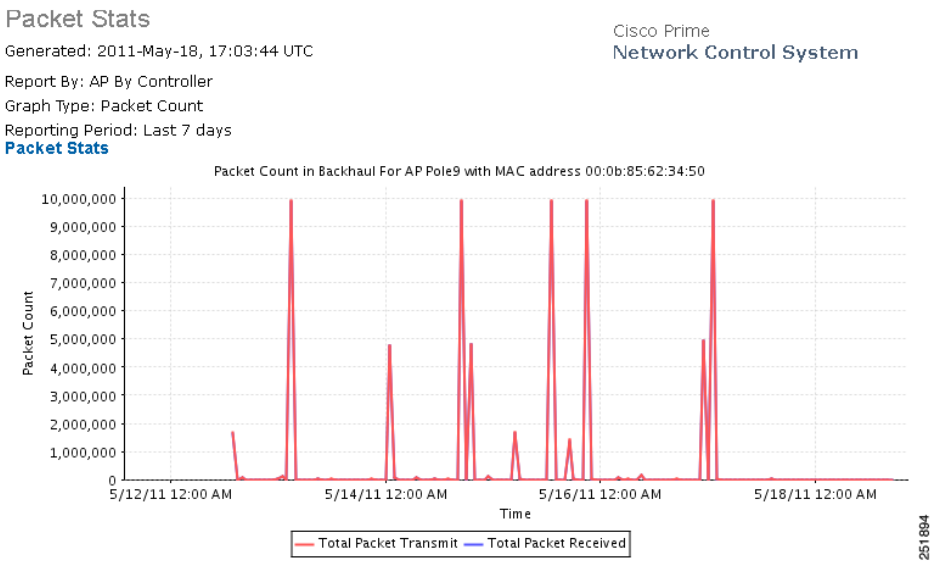
Packet Stats Report Results

The Packet Stats report generates a graph of packet queue statistics for each access point selected and for each report type selected. The graph types are Packet Queue Average, Packets Dropped Per Minute, and Packet Dropped Count.

The following are potential results for a Packet Stats report, depending on how the report is customized (see Figure 14-35):

- Packet Stats
  - Packet Count—Total packets transmitted and total packets received.
  - Packets per Minute—Total packets transmitted per minute and total packets received per minute.
- Packet Error Stats
  - Packet error rate percentages for all neighbor access points or for parent/children neighbor access points only.
- Packet Queue Stats
  - Packet Queue Average—Shows the average number of packets for each queue when the MIB was polled. Silver, gold, platinum, bronze, and management.
  - Packets Dropped Count—Contains the counter for the number of packets dropped.
  - Packets Dropped per Minute—Shows the number of packets dropped since the last sample divided by the number of minutes since the sample.

Figure 14-35 Packet Stats Report Results



Packet Error Statistics

This report notes the percentages of packet errors for packets transmitted by the neighbor mesh access point. The packet error rate percentage is 1 minus the number of successfully transmitted packets/numbers of total packets transmitted.

Configuring a Packet Error Statistics Report

This section describes how to configure a Packet Error Statistics report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report Type—Choose **Packet Error Stats** from the drop-down list.
- Report by—Choose **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to choose specific devices).

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Neighbor Type—Choose **All Neighbors** or **Parent/Children Only**.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.

– From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

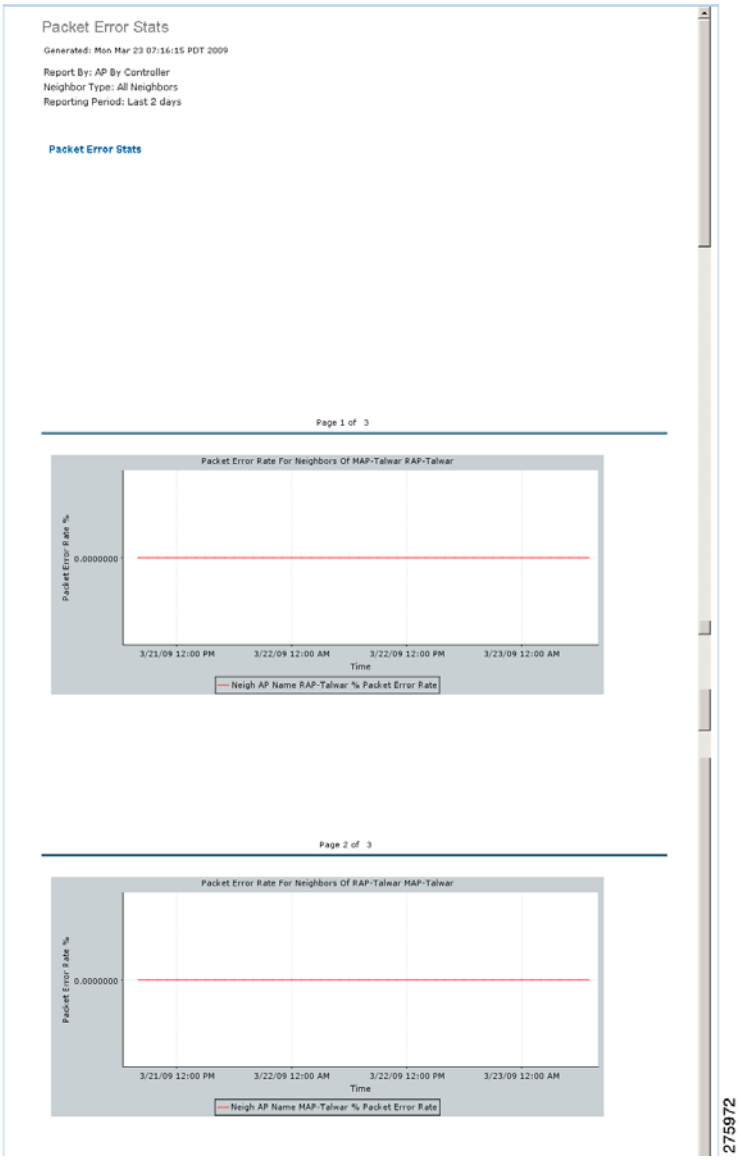
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Packet Error Statistics Report Results

The Packet Error Statistics report contains the following results (Figure 14-36):

Figure 14-36 Packet Error Statistics Report Results



Packet Queue Statistics

This report generates a graph of the total number of packets transmitted and the total number of packets successfully transmitted by the neighbor mesh access point.

Configuring a Packet Queue Statistics Report

This section describes how to configure a Packet Queue Statistics report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report Type—Choose **Packet Queue Stats** from the drop-down list.
- Report by—Choose **AP by Controller**, **AP by Floor Area**, or **AP by Outdoor Area** from the Report by drop-down list and the appropriate selection from the Report Criteria page (or click **Edit** to choose specific devices).

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Graph Type—Choose the type of graph you want displayed for these report results (**Packet Queue Average**, **Packets Dropped Count**, or **Packets Dropped Per Minute**).
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

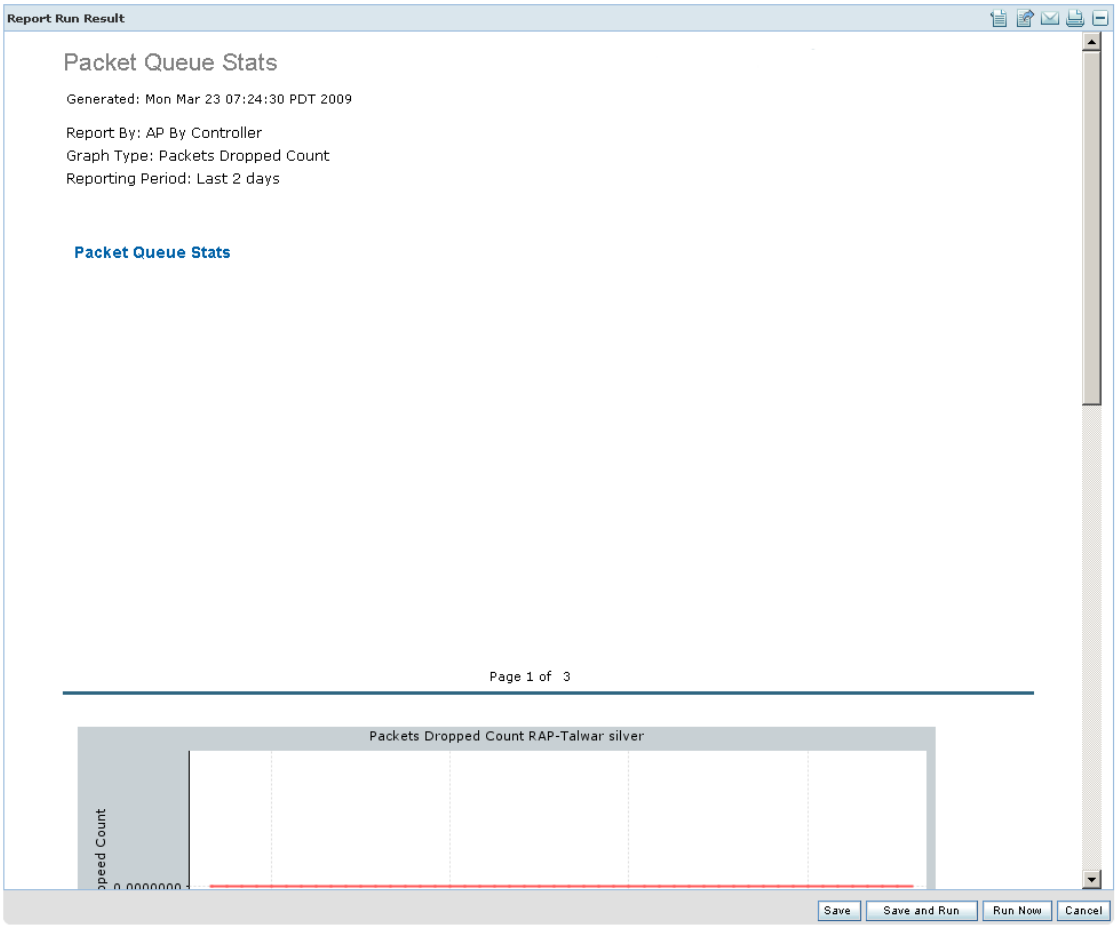
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Packet Queue Statistics Report Results

The Packet Queue Statistics report contains the following results (Figure 14-37):

Figure 14-37 Packet Queue Statistics Report Results



Stranded APs

This report displays access points that appear to be stranded. These access points might have joined a controller at one time and are no longer joined to a controller managed by the NCS, or they might have never joined a controller managed by the NCS.

Click **Stranded APs** from the Report Launch Pad to open the Stranded APs Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Stranded APs Reports page. See the "Configuring a Stranded APs Report" section on page 14-141 and the "Stranded APs Report Results" section on page 14-142 for more information.

Configuring a Stranded APs Report

This section describes how to configure a Stranded APs report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Stranded States—Choose **APs Managed by NCS** or **All**.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Available information for Link Stats report results contain the following:

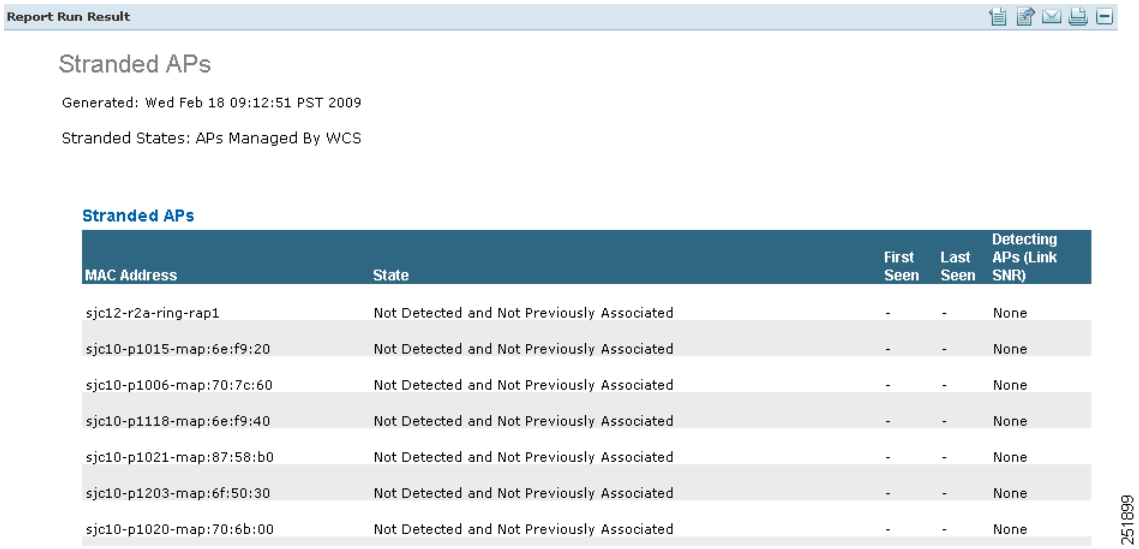
- MAC Address—The MAC address of the stranded access point.
- State—The state of the stranded access point (such as Not Detected and Not Previously Associated).
- First Seen—The date and time this access point was first detected.
- Last Seen—The date and time this access point was last seen.
- Detecting APs (Link SNR)—The access point(s) that detected this stranded access point.

Stranded APs Report Results

The following are potential results for a Stranded APs report, depending on how the report is customized (see Figure 14-38):

- MAC Address (mandatory column)—The MAC address of the stranded access point.
- State (mandatory column)—The state of the stranded access point (such as Not Detected and Not Previously Associated).
- First Seen—The date and time this access point was first detected.
- Last Seen—The date and time this access point was last seen.
- Detecting APs (Link SNR)—The access point(s) that detected this stranded access point.

Figure 14-38 Stranded APs Report Results


Report Run Result

Stranded APs

Generated: Wed Feb 18 09:12:51 PST 2009

Stranded States: APs Managed By WCS

Stranded APs

MAC Address	State	First Seen	Last Seen	Detecting APs (Link SNR)
sjc12-r2a-ring-rap1	Not Detected and Not Previously Associated	-	-	None
sjc10-p1015-map:6e:f9:20	Not Detected and Not Previously Associated	-	-	None
sjc10-p1006-map:70:7c:60	Not Detected and Not Previously Associated	-	-	None
sjc10-p1118-map:6e:f9:40	Not Detected and Not Previously Associated	-	-	None
sjc10-p1021-map:87:58:b0	Not Detected and Not Previously Associated	-	-	None
sjc10-p1203-map:6f:50:30	Not Detected and Not Previously Associated	-	-	None
sjc10-p1020-map:70:6b:00	Not Detected and Not Previously Associated	-	-	None

251899

Worst Node Hops

This report displays the worst node hops or backhaul SNR links for the specified reporting period. The information is displayed in both table and graph form. Report types include worst node hops, worst SNR links for all neighbors, and worst SNR links for parent/children only.

Click **Worst Node Hops** from the Report Launch Pad to open the Worst Node Hops Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Worst Node Hops Reports page. See the "Configuring a Worst Node Hops Report" section on page 14-143 and the "Worst Node Hops Report Results" section on page 14-145 for more information.

Configuring a Worst Node Hops Report

This section describes how to configure a Worst Node Hops report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report Type—Choose **Worst Node Hops** or **Worst SNR Links** from the drop-down list.
- Report Type—When Worst Node Hops is chosen from the Report Type above, choose **Table Only** or **Table and Graph** to determine how the report results display.
- Neighbor Type—When Worst SNR Links is selected from the Report Type, choose **All Neighbors (Table Only)**, **Parent/Children Only (Table Only)**, **All Neighbors (Table and Graph)**, or **Parent/Children Only (Table and Graph)** to determine how the report results display.
- Reporting Period.

- Last—Select the **Last** radio button and choose a period of time from the drop-down list.
- From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Note Worst Node Hops and Worst SNR Links reports are available in both table and graph reports. To customize report results for a particular section, choose the applicable section from the Customizable Report drop-down list.

Worst Node Hops report results contain the following information:

- AP Name—The access point name.
- Node Hops—The number of node hops.
- MAC Address—The MAC address of the access point.
- Parent AP Name—The name of the parent access point.
- Parent MAC Address—The MAC address of the parent access point.
- Time (graph only)—The time of the node hop count.

Available information for Worst SNR Links report results contain the following:

- AP Name—The access point name.
- MAC Address—The MAC address of the access point.
- Neigh SNR—The neighbor signal-to-noise ratio.
- Neigh AP Name—The name of the neighbor access point.
- Neigh MAC Address—The MAC address of the neighbor access point.

- Neigh Type—The neighbor type.
- Time (graph only)—The time of the current report statistics.

Worst Node Hops Report Results

The following are potential results for a Worst Node Hops report, depending on how the report is customized (see Figure 14-39):

- Worst Node Hops report results (table)
  - AP Name (mandatory column).
  - Node Hops (mandatory column)—The number of hops between access points.
  - MAC Address (mandatory column)—The MAC address of the access point.
  - Parent AP Name and MAC Address
- Worst Node Hops report results (graph)
  - Time (mandatory column)—The time of the node hop count.
  - MAC Address (mandatory column)—The MAC address of the access point.
  - Node Hops (mandatory column)—The number of hops between access points.
  - AP Name (mandatory column).
  - Parent AP Name and MAC Address.
- Worst SNR Links report results
  - AP Name (mandatory column).
  - MAC Address (mandatory column in graph report)—The MAC address of the access point.
  - Neighbor SNR (mandatory column).
  - Neighbor AP Name (mandatory column in graph report).
  - Neighbor MAC Address and Type.
  - Time (graph only)(mandatory column)—The time of the current report statistics.

Figure 14-39 Worst Node Hops Report Results

Worst Node Hops

Generated: 2011-May-18, 17:48:34 UTC

Report Type: Table Only

Reporting Period: Last 2 days

Show: Up to 10 records

Cisco Prime
Network Control System

Worst Node Hops Table

AP Name	Node Hops	MAC Address	Parent AP Name
Pole8_b	6	00:0b:85:76:2d:20	Pole10_b
ap:8c:b9:60	6	00:0b:85:8c:b9:60	Pole13_b
Pole13_b	5	00:0b:85:70:6b:30	Pole12
Pole10_b	5	00:0b:85:87:4f:60	Pole13_corner2
ap:8c:b9:60	5	00:0b:85:8c:b9:60	Pole12
Pole19	4	00:0b:85:67:72:d0	Pole19_c2
Pole14-lott	4	00:0b:85:6e:e6:80	Pole19_c2
Pole14_c1	4	00:0b:85:70:6a:b0	Pole19_c2
Pole17	4	00:0b:85:80:e3:90	Pole19_c2

251910

Network Summary

Click **New** for a Network Summary Report type to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

The section describes the Network Summary reports and contains the following topics:

802.11n Summary

This report displays a summary of 802.11n clients and client bandwidth usage for a customizable period of time.

Click **802.11n Summary** from the Report Launch Pad to open the 802.11n Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the 802.11n Summary Reports page. See the "Configuring an 802.11n Summary Report" section on page 14-146 and the "802.11n Summary Report Results" section on page 14-147 for more information.

Configuring an 802.11n Summary Report

This section describes how to configure an 802.11n Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

802.11n Summary Report Results

The following information is displayed for the 802.11n Summary report:

- Number of access points per 802.11n band (pie graph)
- Utilization for 802.11n clients during the specified period of time (line graph)
- Number of associated clients for each protocols during the specified period of time (line graph)

Executive Summary

This report displays a quick view of your wireless network.

Click **Executive Summary** from the Report Launch Pad to open the Executive Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Executive Summary Reports page. See the "Configuring an Executive Summary Report" section on page 14-147 and the "Executive Summary Report Results" section on page 14-147 for more information.

Configuring an Executive Summary Report

This section describes how to configure an Executive Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Executive Summary Report Results

The following information is displayed in the Executive Summary report (see Figure 14-40):

- Number of network devices including access points, controllers, and MSEs.
- Number of LWAPP versus autonomous access points (pie graph).
- Number of associated client in the network during the specified period of time (line graph).

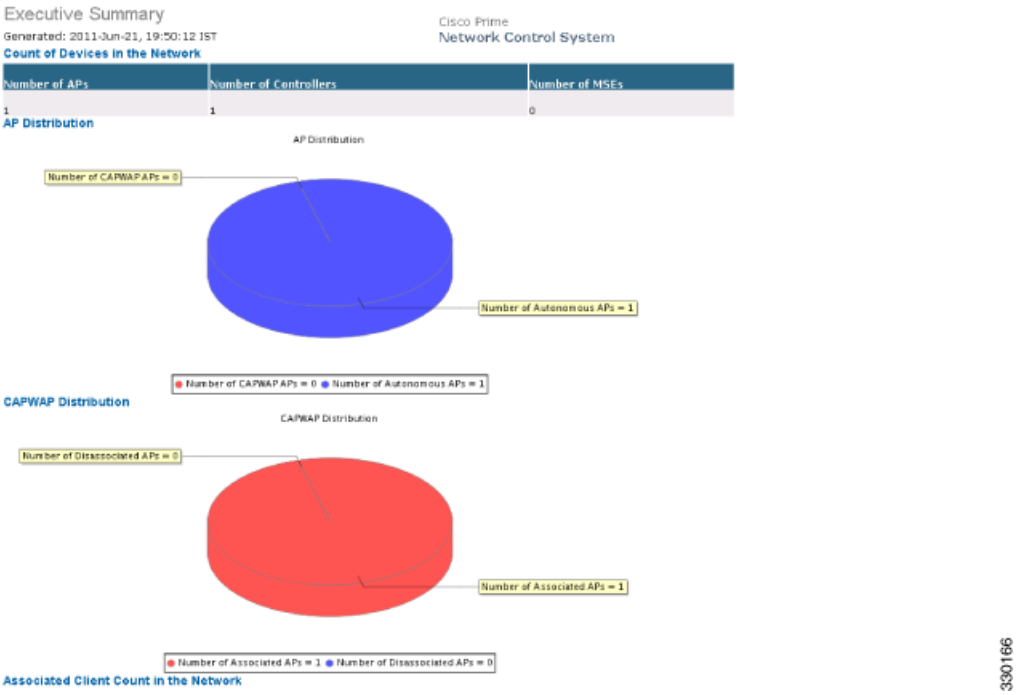
- Number of guest client in the network during the specified period of time (line graph).
- Throughput (Kbps) of clients by protocol during the specified period of time.
- Number of associated clients for each protocol during the specified period of time.
- Network utilization (%) during the specified period of time.
- Air Quality vs Time for each interface.
- Top 10 worst 5 GHz interferers in the network.
- Top 10 worst 2.4 GHz interferers in the network.

Note The Severity 1 refers to the best interferer and Severity 100 refers to the worst interferer in the top 10 worst 5 GHz and 2.4 GHz interferers in the network reports.

Note Executive Summary AP count includes disassociated AP(s) so if you have deleted a controller from the NCS, the CAPWAP count in the report is also reflect the disassociated AP count.

Note The disassociated access points with model and serial number as *null* or *''* values are filtered out from the Executive Summary reports.

Figure 14-40 Executive Summary Report Results



Preferred Calls

This report displays the access points with preferred calls made on the wireless network.

Click **Preferred Calls** from the Report Launch Pad to open the Preferred Calls Reports page. From this page, you can enable, disable, delete, or run currently saved reports. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Executive Summary Reports page. See the "Configuring a Preferred Calls Report" section on page 14-149 and the "Performance Reports" section on page 14-150 for more information.

Configuring a Preferred Calls Report

This section describes how to configure a Preferred Calls report.

Settings

- Report Title—If you plan to use this as a saved report, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to select a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to select a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to select a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Performance Reports

Click **New** for a Performance Report type to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

This section describes the Performance reports and contains the following topics:

802.11 Counters

This report displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retried frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.

Click **802.11 Counters** from the Report Launch Pad to open the 802.11 Counters Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the 802.11 Counters Reports page. See the "Configuring an 802.11 Counters Report" section on page 14-150 and the "802.11 Counters Report Results" section on page 14-152 for more information.

Configuring an 802.11 Counters Report

This section describes how to configure an 802.11 Counters report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

802.11 Counters report results contain the following information:

- Time—The date and time of the count.
- AP Name—The name of the applicable access point.
- Slot—The slot number.
- Radio Type—802.11a/n or 802.11b/g/n.
- Tx Fragment Count—The number of successfully received MPDUs of type Data or Management.
- Rx Fragment Count—The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
- FCS Error Count—The number of FCS errors detected in a received MPDU.
- Retry Count—The number of MSDUs successfully transmitted after one or more retransmissions.
- Multicast Rx Frame Count—The number of MSDUs received with the multicast bit set in the destination MAC address.
- Multicast Tx Frame Count—The number of times a multicast bit is set in the destination MAC address of a successfully transmitted MSDU. Operating as an STA in an ESS, where these frames are directed to the access point, implies having received an acknowledgment to all associated MPDUs.

- Tx Failed Count—The number of MSDUs successfully transmitted after one or more retransmissions.
- Multiple Retry Count—The number of MSDUs successfully transmitted after more than one retransmission.
- Frame Duplicate Count—The number of times a frame is received that the Sequence Control field indicates is a duplicate.
- Tx Frame Count—The number of successfully transmitted MSDUs.
- RTS Success Count—The number of times a CTS is received in response to an RTS.
- RTS Failure Count—The number of times a CTS is not received in response to an RTS.
- ACK Failure Count—The number of times an ACK is not received when expected.
- WEP Undecryptable Count—The number of times a frame is received with the WEP subfield of the Frame Control field set to one and the WEPOn value for the key mapped to the MAC address of the AT indicates that the frame should not have been encrypted or that frame is discarded due to the receiving STA not implementing the privacy option.

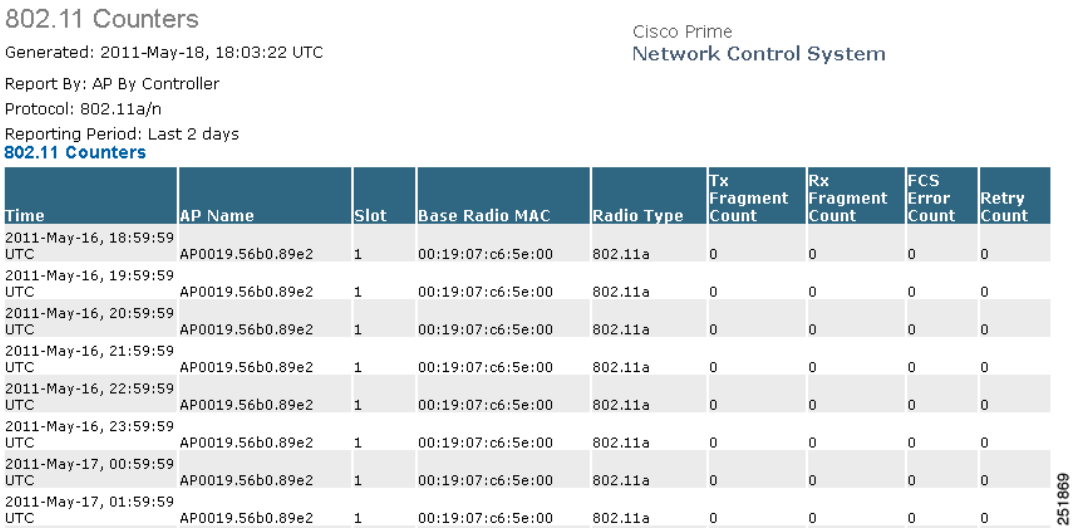
802.11 Counters Report Results

The following are potential results for an 802.11 Counters report, depending on how the report is customized (see Figure 14-41):

- Time (mandatory column)
- AP Name (mandatory column)
- Slot (mandatory column)
- AP MAC Address (mandatory column)
- Radio Type—802.11a/n or 802.11b/g/n.
- Tx Fragment Count—The number of successfully received MPDUs of type Data or Management.
- Rx Fragment Count—The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
- FCS Error Count—The number of FCS errors detected in a received MPDU.
- Retry Count—The number of MSDUs successfully transmitted after one or more retransmissions.
- Multicast Rx Frame Count—The number of MSDUs received with the multicast bit set in the destination MAC address.
- Multicast Tx Frame Count—The number of time a multicast bit is set in the destination MAC address of a successfully transmitted MSDU. When operating as a STA in an ESS, where these frames are directed to the access point, this implies having received an acknowledgment to all associated MPDUs.
- Tx Failed Count—The number of unsuccessful MSDUs transmissions.
- Multiple Retry Count—The number of MSDUs successfully transmitted after more than one retransmission.
- Frame Duplicate Count—The number of times a frame is received that the Sequence Control field indicates is a duplicate.
- Tx Frame Count—The number of successfully transmitted MSDUs.
- RTS Success Count—The number of times a CTS is received in response to an RTS.

- RTS Failure Count—The number of times a CTS is not received in response to an RTS.
- ACK Failure Count—The number of times an ACK is not received when expected.
- WEP Undecryptable Count—The number of times a frame is received with the WEP subfield of the Frame Control field set to one and the WEPOn value for the key mapped to the AT MAC address indicates that the frame should not have been encrypted or that frame is discarded due to the receiving STA not implementing the privacy option.

Figure 14-41 802.11 Counters Report Results



802.11 Counters

Generated: 2011-May-18, 18:03:22 UTC

Cisco Prime
Network Control System

Report By: AP By Controller

Protocol: 802.11a/n

Reporting Period: Last 2 days

802.11 Counters

Time	AP Name	Slot	Base Radio MAC	Radio Type	Tx Fragment Count	Rx Fragment Count	FCS Error Count	Retry Count
2011-May-16, 18:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-16, 19:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-16, 20:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-16, 21:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-16, 22:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-16, 23:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-17, 00:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0
2011-May-17, 01:59:59 UTC	AP0019.56b0.89e2	1	00:19:07:c6:5e:00	802.11a	0	0	0	0

251869

Coverage Hole

This report identifies the location of potential coverage holes in your network and whether they occur more frequently at a given spot. This report can help you modify RRM settings or determine if additional access points are needed to provide coverage in sparsely deployed areas. It runs on the alarm table and shows both the alarm generation time, the cleared time (if cleared), and the state of the alarm (active or cleared).

Click **Coverage Hole** from the Report Launch Pad to open the Coverage Hole Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Coverage Hole Reports page. See the "Configuring a Coverage Hole Report" section on page 14-153 and the "Coverage Hole Report Results" section on page 14-155 for more information.

Configuring a Coverage Hole Report

This section describes how to configure a Coverage Hole report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.

- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Coverage Hole report results contain the following information:

- Time—The date and time the coverage hole was detected.
- State—Clear or Active.
- AP Base Radio MAC Address—The MAC address of the access point base radio.
- AP Name—The name of the access point on which the coverage hole was detected.
- Radio Type—802.11a/n or 802.11b/g/n.
- Failed Clients.
- Total Clients.
- Threshold RSSI.
- Worst Client MAC.

- Worst Client RSSI.

Coverage Hole Report Results

The following are potential results for a Coverage Hole report, depending on how the report is customized (see Figure 14-42):

- Time (mandatory column)—Indicates the date and time that the alarm was generated or cleared (depending on the current state).
- State (mandatory column)—Active or cleared.
- AP Name (mandatory column)—The name of the access point on which the coverage hole was detected.
- Radio Type (mandatory column)—802.11a/n or 802.11b/g/n.
- AP Base Radio MAC Address.
- Failed Clients—The number of clients that have failed due to coverage hole issues.
- Total Clients—The number of total clients associated to this access point.
- Threshold RSSI—The lowest Received Signal Strength Indicator limit.
- Worst Client MAC—The MAC address of the client most affected by coverage hole issues.
- Worst Client RSSI—The Received Signal Strength Indicator of the client most affected by coverage hole issues.

Figure 14-42 Coverage Hole Report Results

Coverage Hole

Generated: 2011-May-18, 18:06:33 UTC

Report By: AP By Controller

Reporting Period: Last 1 day

Cisco Prime
Network Control System

Coverage Holes in the Network

notificationTimestamp	State	AP Name	Radio Type	Failed Clients	Total Clients	Worst Client RSSI
2011-May-18, 14:46:55 UTC	Clear	SJC11-11A-AP3-P099	802.11b/g	0	0	0
2011-May-17, 19:19:14 UTC	Active	SJC11-11A-AP3-P099	802.11b/g	1	1	-82
2011-May-17, 19:20:47 UTC	Clear	SJC11-11A-AP3-P099	802.11b/g	0	0	0
2011-May-17, 19:22:21 UTC	Active	SJC11-11A-AP3-P099	802.11b/g	1	1	-84
2011-May-17, 19:23:54 UTC	Clear	SJC11-11A-AP3-P099	802.11b/g	0	0	0
2011-May-17, 19:42:36 UTC	Active	SJC11-11A-AP3-P099	802.11b/g	1	1	-81
2011-May-17, 19:48:49 UTC	Clear	SJC11-11A-AP3-P099	802.11b/g	0	0	0
2011-May-17, 19:51:56 UTC	Active	SJC11-11A-AP3-P099	802.11b/g	1	1	-82
2011-May-17, 19:53:30 UTC	Clear	SJC11-11A-AP3-P099	802.11b/g	0	0	0

251882

Network Utilization

This report shows the overall network utilization based on the aggregated port utilization of all controllers on your network. These statistics can help identify current network performance and help with capacity planning for future scalability needs.

Note Average utilization (%) is the percentage of utilization where utilization is calculated as ((Tx+Rx)/Bandwidth).

Click **Network Utilization** from the Report Launch Pad to open the Network Utilization Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Network Utilization Reports page. See the "Configuring a Network Utilization Report" section on page 14-156 and the "Network Utilization Report Results" section on page 14-157 for more information.

Configuring a Network Utilization Report

This section describes how to configure a Network Utilization report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fixed columns appear in blue font and cannot be moved to the Available data fields column.

Network Utilization report results contain the following information:

- Time
- Average Utilization (%)—The average aggregated (totalDeltaBits/bandwidth) on all controllers.
- Average Tx (Mbps)—The average aggregated received Mbps of all ports on all controllers.
- Average Rx (Mbps)—The average aggregated (totalDeltaBits/bandwidth) on all controllers.

Network Utilization Report Results

Network utilization is based on the average utilization of all the controllers in the network.

The following information is displayed for a Network Utilization report (see Figure 14-43):

- Time (mandatory column)
- Average Utilization (%) (mandatory column)—Average aggregated (totalDeltaBits/bandwidth) on all controllers.

Note Average utilization (%) is the percentage of utilization where utilization is calculated as ((Tx+Rx)/Bandwidth).

- Average Transmitting (in Mbps)—Average aggregated transmitted Megabytes of all ports on all controllers.
- Average Receiving (in Mbps)—Average aggregated received Megabytes of all ports on all controllers.

Figure 14-43 Network Utilization Report Results

Network Utilization

Generated: 2011-May-18, 18:08:30 UTC

Cisco Prime
Network Control System

Reporting Period: Last 2 days

Network Utilization

Network utilization is based on the average utilization of all the controllers in the network.

Time	Average Utilization (%)	Average Tx (Mbps)	Average Rx (Mbps)
2011-May-16, 18:59:59 UTC	0.09	0.48	0.45
2011-May-16, 19:59:59 UTC	0.10	0.45	0.48
2011-May-16, 20:59:59 UTC	0.10	0.49	0.59
2011-May-16, 21:59:59 UTC	0.11	0.50	0.51
2011-May-16, 22:59:59 UTC	0.08	0.44	0.47
2011-May-16, 23:59:59 UTC	0.12	0.58	0.66
2011-May-17, 00:59:59 UTC	0.09	0.44	0.49
2011-May-17, 01:59:59 UTC	0.08	0.44	0.41
2011-May-17, 02:59:59 UTC	0.08	0.44	0.43

251746

Traffic Stream Metrics

This report can be useful in determining the current and historical quality of service (QoS) for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.

Click **Traffic Stream Metrics** from the Report Launch Pad to open the Traffic Stream Metrics Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Traffic Stream Metrics Reports page. See the "Configuring a Traffic Stream Metrics Report" section on page 14-158 and the "Traffic Stream Metrics Report Results" section on page 14-159 for more information.

Configuring a Traffic Stream Metrics Report

This section describes how to configure a Traffic Stream Metrics report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

The Customize Report Form allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Traffic Stream Metrics report results contain the following information:

- Time—Date and time the statistics were recorded.
- MAC address—The MAC address of the access point.
- AP Name—The access point name.

- Radio Type—802.11a/n or 802.11b/g/n.
- Average Queuing Delay (Downlink)—The average queuing delay for downlinks.
- Average Queuing Delay (Uplink)—The average queuing delay for uplinks.
- % Packet with less than 10 ms delay (downlink)—The percentage of packets that have a queuing delay of less than 10 milliseconds for a downlink.
- % Packet with less than 10 ms delay (uplink)—The percentage of packets that have a queuing delay of less than 10 milliseconds for an uplink.
- % Packet with more than 10 < 20 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 10 but less than 20 milliseconds for a downlink.
- % Packet with more than 10 < 20 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 10 but less than 20 milliseconds for an uplink.
- % Packet with more than 20 < 40 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 20 but less than 40 milliseconds for a downlink.
- % Packet with more than 20 < 40 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 20 but less than 40 milliseconds for an uplink.
- % Packet with more than 40 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 40 milliseconds for a downlink.
- % Packet with more than 40 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 40 milliseconds for an uplink.
- Packet Loss Ratio (Downlink)—The ratio of lost packets for downlinks.
- Packet Loss Ratio (Uplink)—The ratio of lost packets for uplinks.
- Total Packet Count (Downlink)—The total number of downlink packets.
- Total Packet Count (Uplink)—The total number of uplink packets.
- Roaming Count—Number of packets exchanged for roaming negotiations in this 90-second metrics page.
- Roaming Delay—Roaming delay in milliseconds.

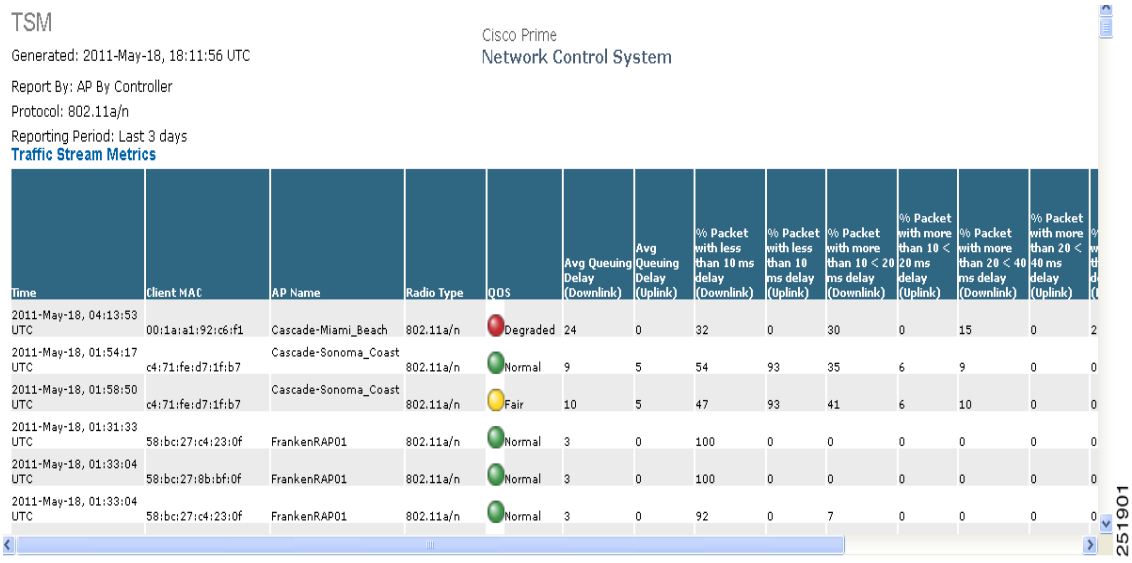
Traffic Stream Metrics Report Results

The following are potential results for a Traffic Stream Metrics report, depending on how the report is customized (see Figure 14-44):

- Time (mandatory column).
- MAC Address (mandatory column).
- AP Name (mandatory column).
- Radio Type (mandatory column).
- Average Queuing Delay (Downlink) (mandatory column).
- Average Queuing Delay (Uplink) (mandatory column).
- % Packet with less than 10 ms delay (downlink)—The percentage of packets that have a queuing delay of less than 10 milliseconds for a downlink.
- % Packet with less than 10 ms delay (uplink)—The percentage of packets that have a queuing delay of less than 10 milliseconds for an uplink.

- % Packet with more than 10 < 20 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 10 but less than 20 milliseconds for a downlink.
- % Packet with more than 10 < 20 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 10 but less than 20 milliseconds for an uplink.
- % Packet with more than 20 < 40 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 20 but less than 40 milliseconds for a downlink.
- % Packet with more than 20 < 40 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 20 but less than 40 milliseconds for an uplink.
- % Packet with more than 40 ms delay (downlink)—The percentage of packets that have a queuing delay of more than 40 milliseconds for a downlink.
- % Packet with more than 40 ms delay (uplink)—The percentage of packets that have a queuing delay of more than 40 milliseconds for an uplink.
- Packet Loss Ratio (Downlink)—The ratio of lost packets for downlinks.
- Packet Loss Ratio (Uplink)—The ratio of lost packets for uplinks.
- Total Packet Count (Downlink)—The total number of downlink packets.
- Total Packet Count (Uplink)—The total number of uplink packets.
- Roaming Count—Number of packets exchanged for roaming negotiations in this 90 seconds metrics page.
- Roaming Delay—Roaming delay in milliseconds.

Figure 14-44 Traffic Stream Metrics Report Results


TSM

Generated: 2011-May-18, 18:11:56 UTC

Report By: AP By Controller

Protocol: 802.11a/n

Reporting Period: Last 3 days

Cisco Prime
Network Control System

Traffic Stream Metrics

Time	Client MAC	AP Name	Radio Type	QOS	Avg Queuing Delay (Downlink)	Avg Queuing Delay (Uplink)	% Packet with less than 10 ms delay (Downlink)	% Packet with less than 10 ms delay (Uplink)	% Packet with more than 10 < 20 ms delay (Downlink)	% Packet with more than 10 < 20 ms delay (Uplink)	% Packet with more than 20 < 40 ms delay (Downlink)	% Packet with more than 20 < 40 ms delay (Uplink)	%
2011-May-18, 04:13:53 UTC	00:1a:a1:92:c6:f1	Cascade-Miami_Beach	802.11a/n	Degraded	24	0	32	0	30	0	15	0	2
2011-May-18, 01:54:17 UTC	c4:71:fe:d7:1f:b7	Cascade-Sonoma_Coast	802.11a/n	Normal	9	5	54	93	35	6	9	0	0
2011-May-18, 01:58:50 UTC	c4:71:fe:d7:1f:b7	Cascade-Sonoma_Coast	802.11a/n	Fair	10	5	47	93	41	6	10	0	0
2011-May-18, 01:31:33 UTC	58:bc:27:c4:23:0f	FrankenRAP01	802.11a/n	Normal	3	0	100	0	0	0	0	0	0
2011-May-18, 01:33:04 UTC	58:bc:27:8b:bf:0f	FrankenRAP01	802.11a/n	Normal	3	0	100	0	0	0	0	0	0
2011-May-18, 01:33:04 UTC	58:bc:27:c4:23:0f	FrankenRAP01	802.11a/n	Normal	3	0	92	0	7	0	0	0	0

251901

Tx Power and Channel

This report displays the channel plan assignment and transmit power level trends of devices based on the filtering criteria used when the report was generated. It helps to identify unexpected behavior or issues with network performance.

Click **Tx Power and Channel** from the Report Launch Pad to open the Tx Power and Channel Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Tx Power and Channel Reports page. See the "Configuring a Tx Power and Channel Report" section on page 14-161 and the "Tx Power and Channel Report Results" section on page 14-161 for more information.

Configuring a Tx Power and Channel Report

This section describes how to configure a Tx Power and Channel report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

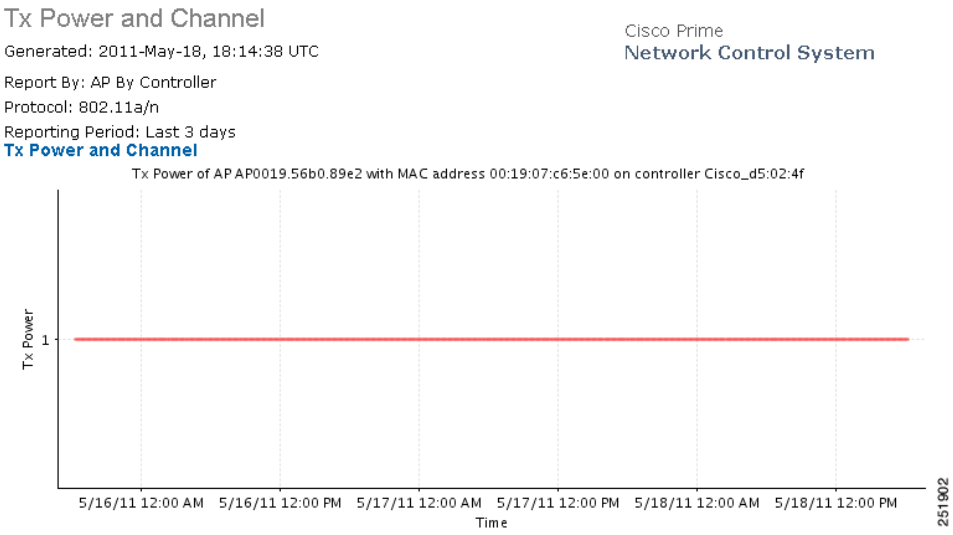
Tx Power and Channel Report Results

The following information is displayed for a Tx Power and Channel report (see Figure 14-45):

- Transmit power level for each access point during the specified period of time.

- Channel number for each access point during the specified period of time.

Figure 14-45 Tx Power and Channel Report Results



VoIP Calls Graph

This report helps analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. To be able to gather useful data from this report, VoIP snooping must be enabled on the WLAN. This report displays information in a graph.

Click **VoIP Calls Graph** from the Report Launch Pad to open the VoIP Calls Graph Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the VoIP Calls Graph Reports page. See the "Configuring a VoIP Calls Graph Report" section on page 14-162 and the "VoIP Calls Report Results" section on page 14-163 for more information.

Configuring a VoIP Calls Graph Report

This section describes how to configure a VoIP Calls Graph report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

- AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

VoIP Calls Report Results

The following information is displayed for a VoIP Calls Graph report:

- Number of attempted VoIP calls per radio during the specified period of time.
- Duration (in seconds) of VoIP calls.

VoIP Calls Table

This report helps analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. To be able to gather useful data from this report, VoIP snooping must be enabled on the WLAN. This report displays information in a table.

Click **VoIP Calls Table** from the Report Launch Pad to open the VoIP Calls Table Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the VoIP Calls Table Reports page. See the "Configuring a VoIP Calls Table Report" section on page 14-163 and the "VoIP Calls Table Results" section on page 14-164 for more information.

Configuring a VoIP Calls Table Report

This section describes how to configure a VoIP Calls Table report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

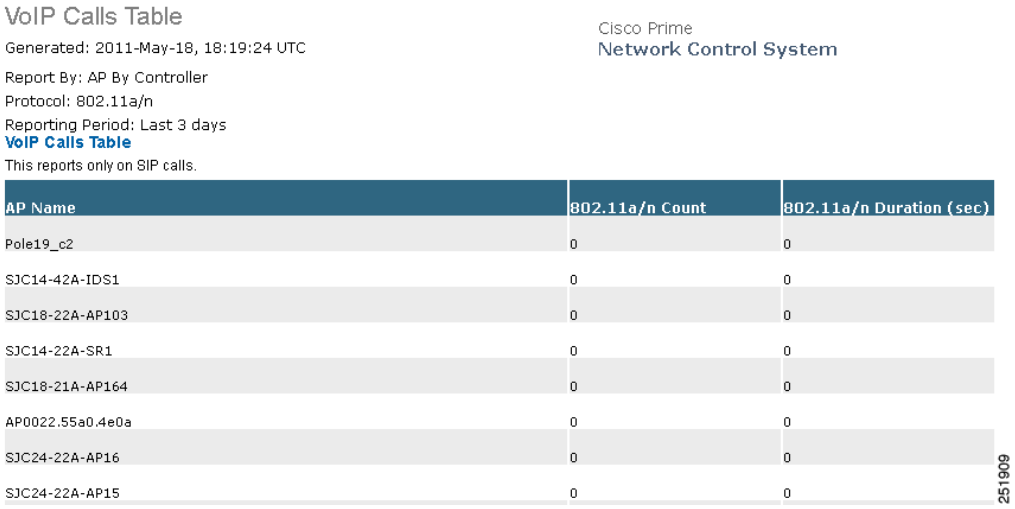
VoIP Calls Table Results

This report displays the same information as the VoIP Calls Graph report but the information is displayed in a table instead of a graph.

The following information is displayed for a VoIP Calls Table report (see Figure 14-46):

- Number of attempted VoIP calls per radio during the specified period of time.
- Duration (in seconds) of VoIP calls.

Figure 14-46 VoIP Calls Table Results



VoIP Calls Table

Generated: 2011-May-18, 18:19:24 UTC

Report By: AP By Controller

Protocol: 802.11a/n

Reporting Period: Last 3 days

VoIP Calls Table

This reports only on SIP calls.

Cisco Prime
Network Control System

AP Name	802.11a/n Count	802.11a/n Duration (sec)
Pole19_c2	0	0
SJC14-42A-IDS1	0	0
SJC18-22A-AP103	0	0
SJC14-22A-SR1	0	0
SJC18-21A-AP164	0	0
AP0022.55a0.4e0a	0	0
SJC24-22A-AP16	0	0
SJC24-22A-AP15	0	0

251909

Voice Statistics

This report helps analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network. To be able to gather useful data from this report, make sure Call Admission Control (CAC) is supported on voice clients.

Note Voice Statistics reports only apply to clients that support Call Admission Control (CAC) and have CAC enabled.

Click **Voice Statistics** from the Report Launch Pad to open the Voice Statistics Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Voice Statistics Reports page. See the "Configuring a Voice Statistics Report" section on page 14-165 and the "Voice Statistics Results" section on page 14-166 for more information.

Configuring a Voice Statistics Report

This section describes how to configure a Voice Statistics report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

- AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
- AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Protocol—Choose **802.11 a/n**, **802.11 b/g/n**, or both.
- Reporting Period
  - Last—Select the **Last** radio button and a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

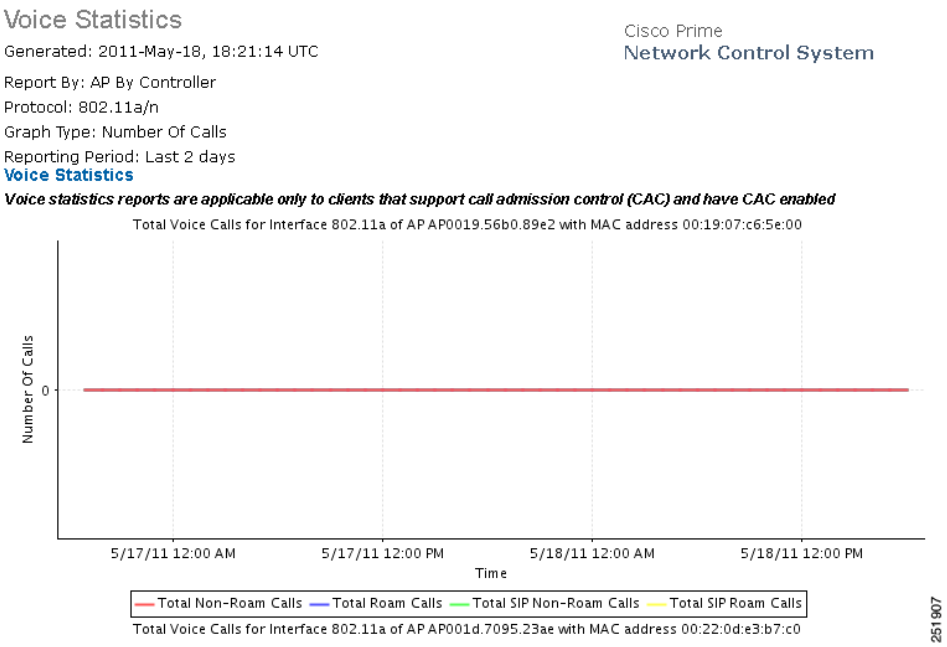
Voice Statistics Results

Note Voice Statistics reports only apply to clients that support Call Admission Control (CAC) and have CAC enabled.

The following information is displayed for a Voice Statistics report (see Figure 14-47):

- Percentage of bandwidth in use during the specified period of time.
- Total number of non-roaming and roaming calls during the specified period of time.
- Number of rejected calls during the specified period of time. Statistics include the following:
  - Total number of rejected calls.
  - Number of rejected roaming and non-roaming calls.
  - Number of rejected calls due to insufficient bandwidth, bad parameters, physical rate, and QoS policy.

Figure 14-47 Voice Statistics Results



Security Reports

Click **New** for a Security Report type to create a new report. See the "Creating and Running a New Report" section on page 14-6 for more information.

Click a report type to view currently saved report templates. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

This section describes the Security reports and contains the following topics:

Adaptive wIPS Alarm

This report displays wIPS alarms by selected MSEs, controllers, and access points for each alarm type.

Click **Adaptive wIPS Alarms** from the Report Launch Pad to open the Adaptive wIPS Alarms Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Adaptive wIPS Alarms Reports page. See the "Configuring an Adaptive wIPS Alarm Report" section on page 14-168 and the "Adaptive wIPS Alarm Report Results" section on page 14-169 for more information.

Configuring an Adaptive wIPS Alarm Report

This section describes how to configure an Adaptive wIPS Alarms report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - MSE with Adaptive wIPS Service—Choose **All MSEs with Adaptive wIPS Service** from the Report Criteria drop-down list, or click **Edit** to choose a specific MSE.
  - Controller by MSE—Choose **All MSEs > All Controllers** from the Report Criteria drop-down list, or click **Edit** to choose a specific controller.
  - AP by MSE—Choose **All MSEs > All Controllers > All APs** from the Report Criteria drop-down list, or click **Edit** to choose a specific access point.

Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Alarm Category—Choose **All Types**, **Denial of Service (DoS)**, or **Security Penetration** to determine the types of wIPS alarms to display in the results.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The reporting period is based on the time that the alarm was last seen. The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

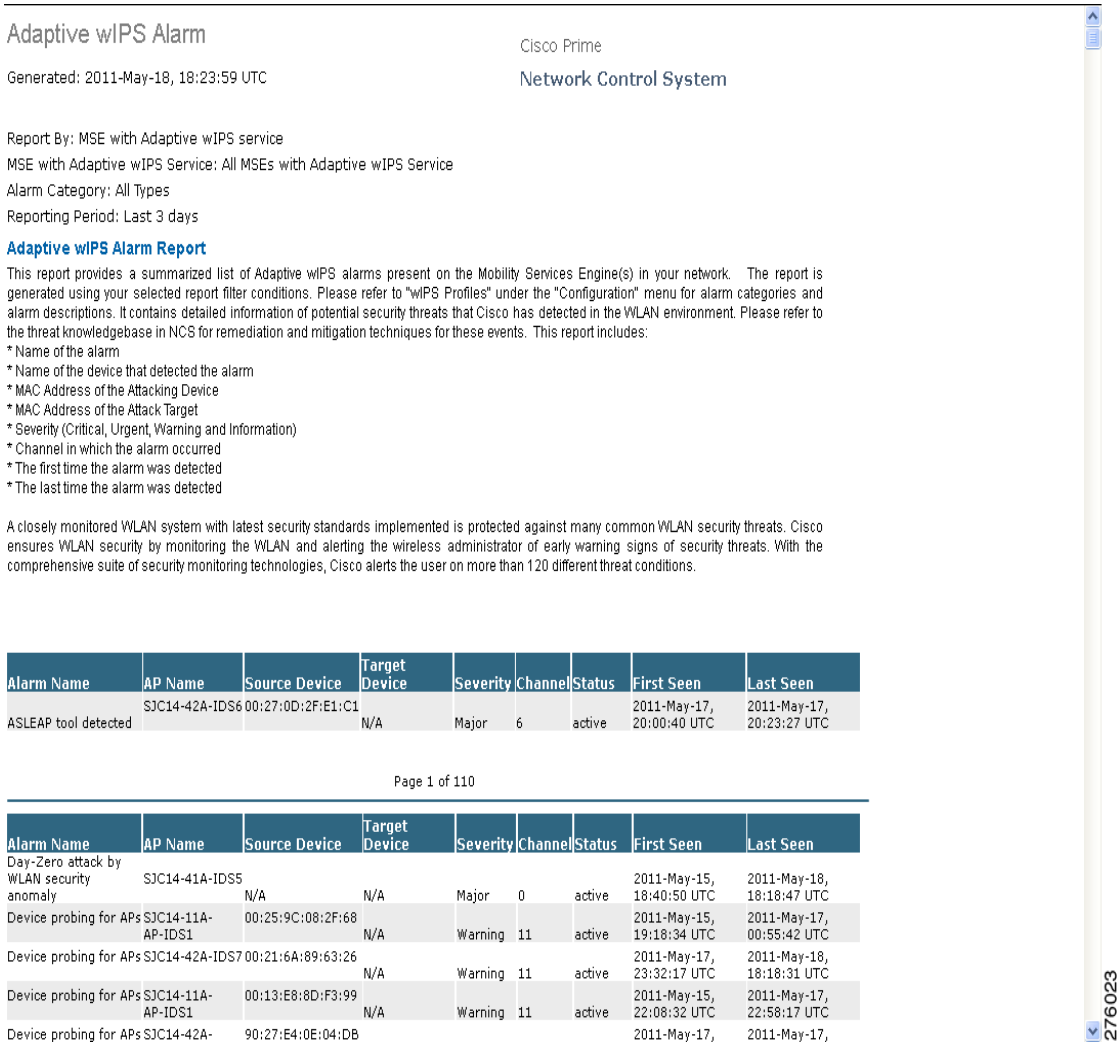
Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Adaptive wIPS Alarm Report Results

An Adaptive wIPS Alarm Report potentially contains the following information, depending on how the report is customized (see Figure 14-48):

- Alarm Name (mandatory column).
- AP Name—The name of the device that detected the alarm.
- Source Device—Identifies the device that initiated the potential attack.
- Target Device—Identifies the device targeted by the potential attack.
- Severity—Indicates the severity of the attack (Critical, Urgent, Warning, Information).
- Channel—The channel on which the alarm occurred.
- Status—The current status of the alarm (Active or Inactive).
- First Seen—The date and time the alarm was first detected.
- Last Seen—The date and time the alarm was last detected.
- AP MAC Address—The MAC address of this access point.
- Target SSID—The Service Set Identifier of the targeted device.
- Alarm Category.
- MSE Name—The name of the MSE to which this device is associated.

Figure 14-48 Adaptive wIPS Alarms Report



Adaptive wIPS Alarm

Cisco Prime
Network Control System

Generated: 2011-May-18, 18:23:59 UTC

Report By: MSE with Adaptive wIPS service
MSE with Adaptive wIPS Service: All MSEs with Adaptive wIPS Service
Alarm Category: All Types
Reporting Period: Last 3 days

Adaptive wIPS Alarm Report

This report provides a summarized list of Adaptive wIPS alarms present on the Mobility Services Engine(s) in your network. The report is generated using your selected report filter conditions. Please refer to "wIPS Profiles" under the "Configuration" menu for alarm categories and alarm descriptions. It contains detailed information of potential security threats that Cisco has detected in the WLAN environment. Please refer to the threat knowledgebase in NCS for remediation and mitigation techniques for these events. This report includes:
* Name of the alarm
* Name of the device that detected the alarm
* MAC Address of the Attacking Device
* MAC Address of the Attack Target
* Severity (Critical, Urgent, Warning and Information)
* Channel in which the alarm occurred
* The first time the alarm was detected
* The last time the alarm was detected

A closely monitored WLAN system with latest security standards implemented is protected against many common WLAN security threats. Cisco ensures WLAN security by monitoring the WLAN and alerting the wireless administrator of early warning signs of security threats. With the comprehensive suite of security monitoring technologies, Cisco alerts the user on more than 120 different threat conditions.

Alarm Name	AP Name	Source Device	Target Device	Severity	Channel	Status	First Seen	Last Seen
ASLEAP tool detected	SJC14-42A-IDS6	00:27:0D:2F:E1:C1	N/A	Major	6	active	2011-May-17, 20:00:40 UTC	2011-May-17, 20:23:27 UTC

Page 1 of 110

Alarm Name	AP Name	Source Device	Target Device	Severity	Channel	Status	First Seen	Last Seen
Day-Zero attack by WLAN security anomaly	SJC14-41A-IDS5	N/A	N/A	Major	0	active	2011-May-15, 18:40:50 UTC	2011-May-18, 18:18:47 UTC
Device probing for APs	SJC14-11A-AP-IDS1	00:25:9C:08:2F:68	N/A	Warning	11	active	2011-May-15, 19:18:34 UTC	2011-May-17, 00:55:42 UTC
Device probing for APs	SJC14-42A-IDS7	00:21:6A:89:63:26	N/A	Warning	11	active	2011-May-17, 23:32:17 UTC	2011-May-18, 18:18:31 UTC
Device probing for APs	SJC14-11A-AP-IDS1	00:13:E8:8D:F3:99	N/A	Warning	11	active	2011-May-15, 22:08:32 UTC	2011-May-17, 22:58:17 UTC
Device probing for APs	SJC14-42A-	90:27:E4:0E:04:DB					2011-May-17,	2011-May-17,

276023

Adaptive wIPS Alarm Summary

This report displays a summary of all the Adaptive wIPS Alarms on your network.

Click **Adaptive wIPS Alarm Summary** from the Report Launch Pad to open the Adaptive wIPS Alarm Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Adaptive wIPS Alarm Summary Reports page. See the "Configuring an Adaptive wIPS Alarm Summary Report" section on page 14-170 and the "Adaptive wIPS Alarm Summary Report Results" section on page 14-171 for more information.

Configuring an Adaptive wIPS Alarm Summary Report

This section describes how to configure an Adaptive wIPS Alarm Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By
  - MSE with Adaptive wIPS Service—Choose **All MSEs with Adaptive wIPS Service** from the Report Criteria drop-down list or click **Edit** to choose a specific MSE.
  - Controller by MSE—Choose **All MSEs > All Controllers** from the Report Criteria drop-down list or click **Edit** to choose a specific controller.
  - AP by MSE—Choose **All MSEs > All Controllers > All APs** from the Report Criteria drop-down list or click **Edit** to choose a specific access point.

Note In the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Alarm Category—Choose **All Types**, **Denial of Service (DoS)**, or **Security Penetration** to determine the types of wIPS alarms to be displayed in the results.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The reporting period is based on the time that the alarm was last seen. The times are shown in the local time of the NCS server.

- Show—Enter the number of records that you want displayed in the report.

Note Enter a number between 5 and 1000, or leave the text box blank to display all records.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information about customizing report results.

Note Data fields that appear in blue font cannot be removed from the list of fields to be included.

Adaptive wIPS Alarm Summary Report Results

An Adaptive wIPS Alarm Summary Report potentially contains the following information, depending on how the report is customized (see Figure 14-49):

- Alarm Name (mandatory column)

- Category—Alarm category
- Severity Information
  - Critical—The number of critical alarms for this access point.
  - Major—The number of major alarms for this access point.
  - Minor—The number of minor alarms for this access point.
  - Warning—The number of warning alarms for this access point.
- Total—The number of total alarms for this access point.

Figure 14-49 Adaptive wIPS Alarm Summary Report

Adaptive wIPS Alarm Summary

Generated: 2011-May-18, 18:28:19 UTC

Cisco Prime
Network Control System

Report By: MSE with Adaptive wIPS service
MSE with Adaptive wIPS Service: All MSEs with Adaptive wIPS Service
Alarm Category: All Types
Reporting Period: Last 3 days
Show: Up to 10 records

Page 1 of 3

Adaptive wIPS Alarm Summary Report

This report provides a consolidated list of all the alarms categories (Security IDS/IPS and Performance Intrusion) that have occurred in the WLAN environment. An insecure network can usually be fixed by reconfiguring some of the network equipment, by using additional software or hardware and always being in the forefront of implementing the latest security standards to provide good security for sensitive data such as employee salary data or company financial information. A closely monitored and well tuned WLAN system can achieve a higher throughput than a poorly managed one. AirMagnet ensures WLAN performance and efficiency by monitoring the WLAN and alerting the wireless administrator on early warning signs for trouble. This includes reporting the devices which are vulnerable to violations/are violating and actions that can be performed to nullify such violations. With the comprehensive suite of security monitoring technologies, Cisco alerts the user on more 50 different threat conditions. The report includes the different types of policy violations categories, the number of times they have occurred and also breaks it down to the severity level (Critical, Major, Minor and Warning). Please refer to the Configure>wIPS Profiles to view all the possible alarm categories. threat knowledgebase in NCS for remediation and mitigation techniques for these events. A closely monitored WLAN system with latest security standards implemented is protected against many common WLAN security threats. Cisco ensures WLAN security by monitoring the WLAN and alerting the wireless administrator of early warning signs of security threats. With the comprehensive suite of security monitoring technologies, Cisco alerts the user on more than 120 different threat conditions.This report includes the different types of potential security threats, the number of times they have occurred and also breaks it down to the severity level (Critical, Major, Minor and Warning) for each of the Top 10 APs. Please refer to "wIPS Profiles" under the "Configuration" menu to view all detected alarms and their respective category.

AlarmName	Category	Critical	Major	Minor	Warning	Total
Unauthorized association by vendor list	wIPS - Security Penetration	26455	0	0	0	26455
Suspicious after-hours traffic detected	wIPS - Security Penetration	0	0	25555	0	25555
Spoofed MAC address detected	wIPS - Security Penetration	0	7829	0	0	7829
DoS: CTS flood	wIPS - Denial of Service Attack	6656	0	0	0	6656
DoS: RTS flood	wIPS - Denial of Service Attack	5451	0	0	0	5451
Unauthorized association detected	wIPS - Security Penetration	2711	0	0	0	2711
Malformed 802.11 packets detected	wIPS - Security Penetration	0	2024	0	0	2024

282613

Page 2 of 3

Adaptive wIPS Top 10 AP

This report displays the top ten access points with the highest number of generated Adaptive wIPS alarms.

Click **Adaptive wIPS Top 10 APs** from the Report Launch Pad to open the Adaptive wIPS Top 10 APs Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Adaptive wIPS Top 10 APs Reports page. See the "Configuring an Adaptive wIPS Top 10 AP Report" section on page 14-173 and the "Adaptive wIPS Top 10 AP Report Results" section on page 14-174 for more information.

Configuring an Adaptive wIPS Top 10 AP Report

This section describes how to configure a wIPS Top 10 AP report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By
  - MSE with Adaptive wIPS Service—Choose **All MSEs with Adaptive wIPS Service** from the Report Criteria drop-down list or click **Edit** to choose a specific MSE.
  - Controller by MSE—Choose **All MSEs > All Controllers** from the Report Criteria drop-down list or click **Edit** to choose a specific controller.

Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Alarm Category—Choose **All Types**, **Denial of Service (DoS)**, or **Security Penetration** to determine the types of wIPS alarms to display in the results.

Note See the wIPS Policy Alarm Encyclopedia for more information regarding wIPS alarm types.

- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The reporting period is based on the time that the alarm was last seen. The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Adaptive wIPS Top 10 AP Report Results

An Adaptive wIPS Top 10 AP report potentially contains the following information, depending on how the report is customized (see Figure 14-50):

- AP Name (mandatory column)
- Critical—The number of critical alarms for this access point.
- Major—The number of major alarms for this access point.
- Minor—The number of minor alarms for this access point.
- Warning—The number of warning alarms for this access point.
- Total—The number of total alarms for this access point.
- AP MAC Address—The MAC address of this access point.
- MSE Name—The name of the MSE to which this access point is associated.

Figure 14-50 Adaptive wIPS Top 10 APs Report

Adaptive wIPS Top 10 AP

Generated: 2011-May-18, 18:41:33 UTC

Cisco Prime
Network Control System

Report By: MSE with Adaptive wIPS service
MSE with Adaptive wIPS Service: All MSEs with Adaptive wIPS Service
Alarm Category: All Types
Reporting Period: Last 3 days

Adaptive wIPS Top 10 AP Report

This report provides a list of the top 10 wIPS monitoring APs that have detected the most security alarms that have occurred in the WLAN environment. These alarms are stored on the Mobility Services Engine(s) installed on your network running Adaptive wIPS. A high number of alarms on a monitoring AP is indicative of "security hot spots" in the network that warrant closer investigation. Please refer to the threat knowledgebase in WCS for remediation and mitigation techniques for these events. A closely monitored WLAN system with latest security standards implemented is protected against many common WLAN security threats. Cisco ensures WLAN security by monitoring the WLAN and alerting the wireless administrator of early warning signs of security threats. With the comprehensive suite of security monitoring technologies, Cisco alerts the user on more than 120 different threat conditions.This report includes the different types of potential security threats, the number of times they have occurred and also breaks it down to the severity level (Critical, Major, Minor and Warning) for each of the Top 10 APs. Please refer to "wIPS Profiles" under the "Configuration" menu to view all detected alarms and their respective category.

AP Name	Critical	Major	Minor	Warning	Total
SJC14-11A-AP-IDS1	270	5	36	11	322

Page 1 of 2

275947

Adhoc Rogue Count Summary

This report displays a summarized count of all ad hoc rogue access points.

Click **Adhoc Rogue Count Summary** from the Report Launch Pad to open the Adhoc Rogue Count Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Adhoc Rogue Count Summary Reports page. See the "Configuring an Adhoc Rogue Count Summary Report" section on page 14-175 and the "Adhoc Rogue Count Summary Report Results" section on page 14-176 for more information.

Note You cannot upgrade the Adhoc Rogue Count Summary reports to the NCS Release 1.0 and later.

Configuring an Adhoc Rogue Count Summary Report

This section describes how to configure an Adhoc Rogue Count Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.

  Note In the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Classification Type—Choose **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to be displayed in the report results.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

  Note The reporting period is based on the time that the alarm was last seen. The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

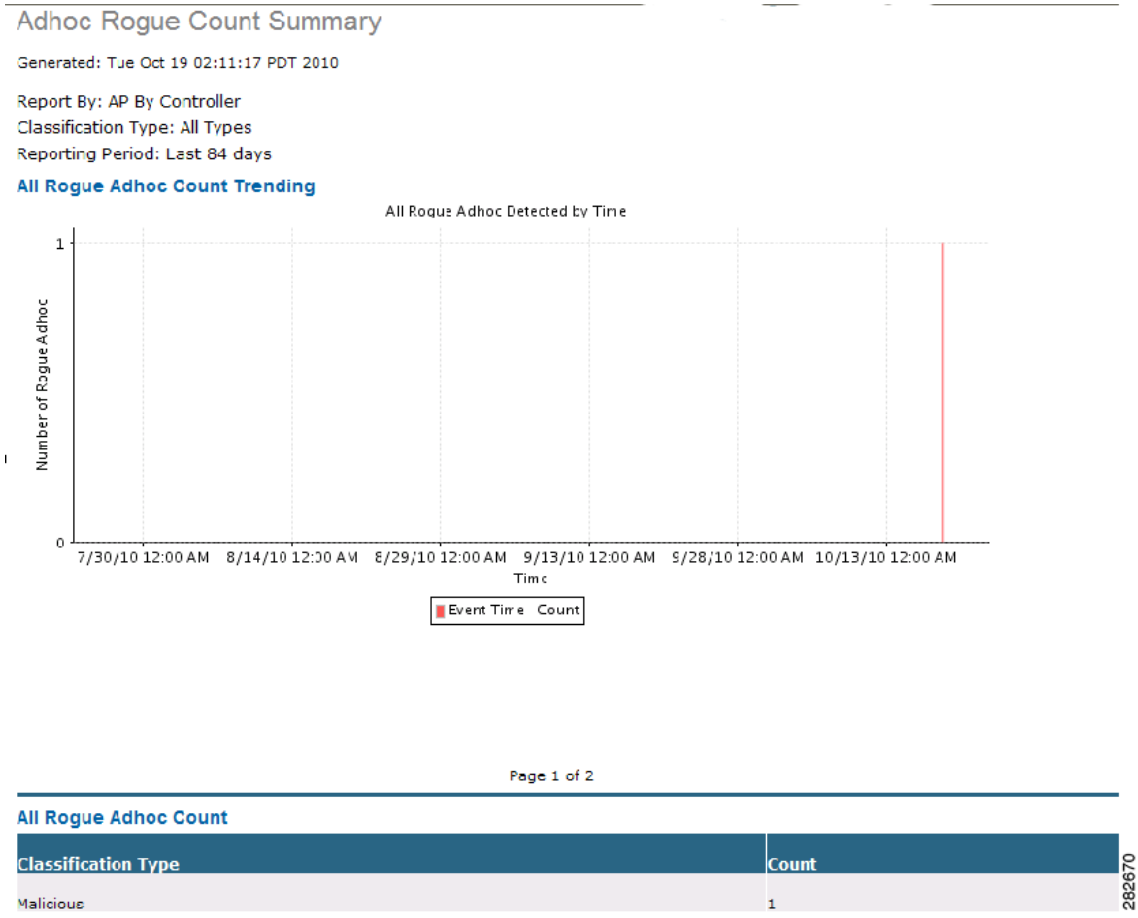
Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information about customizing report results.

Note Data fields that appear in blue font cannot be removed from the list of fields to be included.

Adhoc Rogue Count Summary Report Results

The following are potential results for an Adhoc Rogue Count Summary report, depending on how the report is customized (see Figure 14-51):

Figure 14-51 Adhoc Rogue Count Summary Report



Adhoc Rogue Events

This report displays all ad hoc rogue events received by the NCS.

The following settings and scheduling parameters are available for this report:

Click **Adhoc Rogue Events** from the Report Launch Pad to open the Adhoc Rogue Events Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Adhoc Rogue Events Reports page. See the "Configuring an Adhoc Rogue Events Report" section on page 14-177 and the "Adhoc Rogue Events Report Results" section on page 14-178 for more information.

Configuring an Adhoc Rogue Events Report

Settings

The following settings can be configured for an Adhoc Rogue Events report:

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

  Note From the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period

  Note Reporting period is based on the alarm Last Seen time.

  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Creating a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Export Now—Click to export the report results. The supported export formats is PDF and CSV.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Adhoc Rogue Events Report Results

The following are potential results for an Adhoc Rogue Events report, depending on how the report is customized:

- Last Seen Time (mandatory column)
- Rogue MAC Address (mandatory column)
- Detecting AP Name (mandatory column)
- Radio Type—802.11a or 802.11b/g.
- Controller IP Address—The IP address of the controller on which the adhoc rogue is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the ad hoc rogue was detected.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state relative to the network or port. Ad hoc rogue radios appear as "Alert" when first scanned by the port, or as "Pending" when operating system identification is still underway.
- Channel Number—The channel number of the ad hoc rogue.
- RSSI (dBm)—The Received Signal Strength Indicator in dBm.

Adhoc Rogues

This report displays details for all ad hoc rogue devices detected by your network access points based on the time they were last seen.

The NCS receives updates about ad hoc rogues from controllers by using traps or by polling. Last Seen Time is updated anytime a trap for the ad hoc rogue is received or the ad hoc rogue was seen during the last polling cycle of the NCS.

Note This report includes rogue access point alarms with clear severity.

Click **Adhoc Rogues** from the Report Launch Pad to open the Adhoc Rogues Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Adhoc Rogues Reports page. See the "Configuring an Adhoc Rogues Report" section on page 14-179 and the "Adhoc Rogues Report Results" section on page 14-180 for more information.

Note You cannot upgrade the Adhoc Rogues reports to the NCS Release 1.0 and later.

Configuring an Adhoc Rogues Report

This section describes how to configure an Adhoc Rogues report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.

  Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

  Note The reporting period is based on the time that the alarm was last seen. The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Adhoc Rogues Report Results

The following are potential results for an Adhoc Rogues report, depending on how the report is customized (see Figure 14-52):

- Last Seen Time—Date and time the ad hoc rogue was last seen.
- Detecting AP Name—The access point that last detected the rogue, when a rogue is detected by multiple access points on one controller. This last detected access point name comes from the controller that supports maximum RSSI.
- Radio Type—802.11a/n or 802.11b/g/n.
- Controller IP Address—The IP address of the controller on which the ad hoc rogue is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the ad hoc rogue was detected.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state relative to the network or port. Ad hoc rogue radios appear as “Alert” when first scanned by the port, or as “Pending” when operating system identification is still underway.
- Rogue MAC Address—The MAC address of the ad hoc rogue.
- Channel Number—The channel number of the ad hoc rogue.
- RSSI (dBm)—The maximum Received Signal Strength Indicator ever reported by any controller for this rogue.

Figure 14-52 Adhoc Rogues Results

Adhoc Rogues

Generated: 2011-May-18, 18:50:02 UTC

Report By: AP By Controller

Reporting Period: Last 2 days

Cisco Prime
Network Control System

Adhoc Rogues

Last Seen Time	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Detecting AP Map Location	SSID	State	Severity
2011-May-18, 11:00:43 UTC	1a:9a:dd:87:d1:39	SJC24-31A-AP27	802.11b/g/n	10.32.34.2	System Campus > SJC-24 > 3rd Floor	Brent Mower's Guest Network	Removed	Clear
2011-May-18, 17:16:00 UTC	08:61:08:00:45:00	SJC14-41A-IDS8	802.11b/g/n	10.32.34.2			Alert	Minor
2011-May-18, 17:15:35 UTC	09:47:08:00:45:00	SJC14-41A-ROBERT-MOSES	802.11b/g/n	10.32.34.2			Alert	Minor
2011-May-18, 17:16:08 UTC	06:25:84:09:1e:ee	SJC19-42A-AP207	802.11b/g/n	10.32.34.2	System Campus > SJC-19 > 4th Floor	bb-voice	Alert	Minor
2011-May-18, 17:16:17 UTC	06:25:84:09:23:2a	SJC19-42A-AP207	802.11b/g/n	10.32.34.2	System Campus > SJC-19 > 4th Floor	cisco-32-voice	Alert	Minor
2011-May-18, 17:16:17 UTC	06:25:84:09:22:ce	SJC19-42A-AP207	802.11b/g/n	10.32.34.2	System Campus > SJC-19 > 4th Floor	uc320-voice-acwang	Alert	Minor
2011-May-17, 20:14:49 UTC	8a:43:e1:ab:00:d5	SJC19-42A-AP207	802.11b/g/n	10.32.37.6	System Campus > SJC-19 > 4th Floor	asterisk	Alert	Minor
2011-May-17, 03:28:12 UTC	00:26:4a:da:03:e0	SJC17-31A-P192	802.11b/g	10.34.142.150	System Campus > SJC-17 > 3rd Floor	hpsetup	Removed	Clear
2011-May-18, 17:17:48 UTC	00:16:35:9f:74:d2	SJC17-31A-P197	802.11b/g	10.34.142.150	System Campus > SJC-17 > 3rd Floor	hpsetup	Removed	Clear

251874

New Rogue AP Count Summary

This report displays a summarized count of all the new rogue access points.

Click **New Rogue AP Count Summary** from the Report Launch Pad to open the New Rogue AP Count Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the New Rogue AP Count Summary Reports page. See the "Configuring a New Rogue AP Count Summary Report" section on page 14-181 and the "New Rogue AP Count Summary Report Results" section on page 14-182 for more information.

Note You cannot upgrade the New Rogue AP Count Summary reports to the NCS Release 1.0 and later.

Configuring a New Rogue AP Count Summary Report

This section describes how to configure a New Rogue AP Count Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.

  Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Classification Type—Choose **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to be displayed in the report results.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

  Note The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

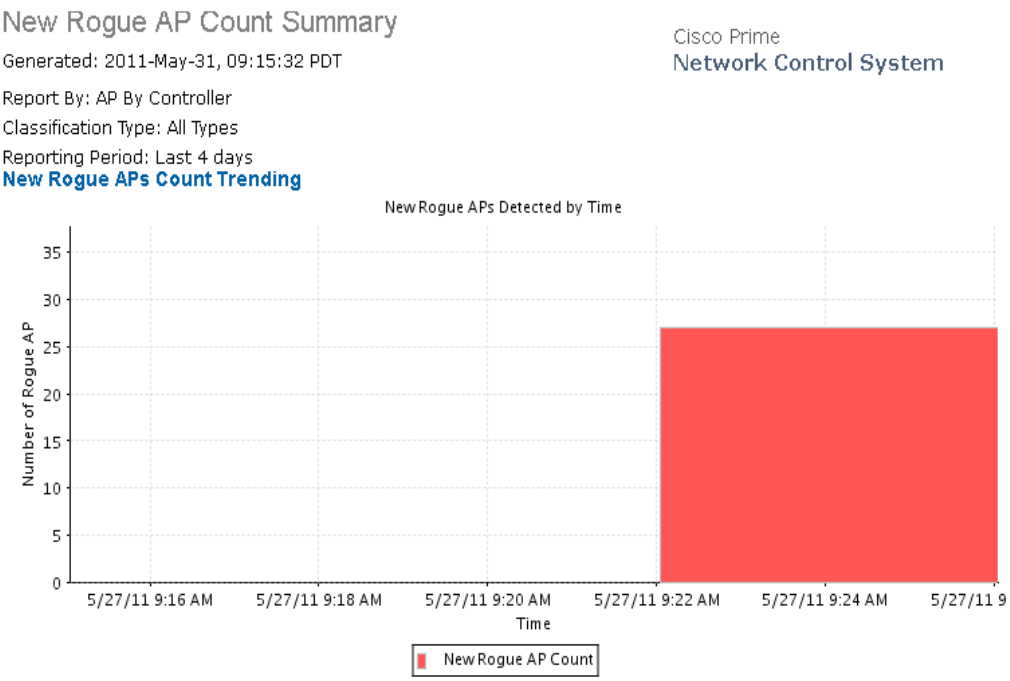
Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information about customizing report results.

Note Data fields that appear in blue font cannot be removed from the list of fields to be included.

New Rogue AP Count Summary Report Results

The following are potential results for a New Rogue AP Count Summary report, depending on how the report is customized (see Figure 14-53):

Figure 14-53 New Rogue AP Count Summary Report



New Rogue APs

This report displays all the new rogues detected for the first time on your network within the selected timeframe for this report. The value in the Created Time column indicates the time at which the rogue was first detected.

Note This report includes rogue access point alarms with clear severity.

Click **New Rogue AP** from the Report Launch Pad to open the New Rogue APs Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the New Rogue APs Reports page. See the "Configuring a New Rogue AP Report" section on page 14-183 and the "New Rogue AP Report Results" section on page 14-183 for more information.

Note You cannot upgrade the New Rogue APs reports to the NCS Release 1.0 and later.

Configuring a New Rogue AP Report

This section describes how to configure a New Rogue Access Points report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.

  Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Classification Type—Choose **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to display in the report results.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

  Note The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

New Rogue AP Report Results

The following are potential results for a New Rogue APs report, depending on how the report is customized (see Figure 14-54):

Note The results for this report are sorted based on First Time Seen.

- First Seen Time—The date and time the rogue access point was first seen.
- Rogue MAC Address—The MAC address of the rogue access point. Click the MAC address link to view the alarm details of the access point.
- Detecting AP Name—The access point that last detected the rogue, when a rogue is detected by multiple access points on one controller. This last detected access point name comes from the controller that supports maximum RSSI.
- Radio Type—802.11a/n or 802.11b/g/n.
- Controller IP Address—The IP address of the controller on which the rogue access point is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the rogue access point was detected.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state relative to the network or port. Rogue access point radios appear as "Alert" when first scanned by the port, or as "Pending" when operating system identification is still underway.
- Channel Number—The channel number of the rogue access point.
- RSSI (dBm)—The Received Signal Strength Indicator in dBm.
- Classification Type—The type of rogue access point (malicious, friendly, or unclassified).
- Switch Port Trace Status—Indicates whether or not the switch port was traced.
- Switch Port Trace Summary—Provides a summary of the switch port trace or remains blank if no switch port was traced.

Figure 14-54 New Rogue Access Points Report

New Rogue APs

Generated: 2011-May-18, 18:57:00 UTC

Report By: AP By Controller

On Network: All Types

Reporting Period: Last 3 days

Cisco Prime
Network Control System

New Rogue APs

First Seen Time	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Detecting AP Map Location	SSID	State	Classification Type	On Network
2011-May-18, 17:15:26 UTC	00:0f:f8:58:52:62	SJC24-11A-AP11	802.11b/g/n	10.32.34.2	System Campus > SJC-24 > 1st Floor	mobilevpn	Alert	Unclassified	No
2011-May-18, 17:15:26 UTC	00:21:d8:7e:73:74	wnbu-bgl11-41a-iap-ap3	802.11b/g	10.65.23.39			Alert	Unclassified	No
2011-May-18, 17:15:26 UTC	00:1f:f3:02:da:cd	supusu-homeap	802.11b/g	171.70.35.135		2WIRE268	Alert	Unclassified	No
2011-May-18, 17:15:26 UTC	00:21:29:bf:6b:74	supusu-homeap	802.11b/g	171.70.35.135		Simba	Alert	Unclassified	No
2011-May-18, 17:15:26 UTC	08:17:35:c7:2c:8d	dwill-homeap	802.11a	171.70.35.135		Cisco-.1x	Alert	Unclassified	No
2011-May-18, 17:15:26 UTC	08:17:35:c7:2c:8c	dwill-homeap	802.11a	171.70.35.135		Cisco-open	Alert	Unclassified	No
2011-May-18, 17:15:26 UTC	08:17:35:c7:02:4d	dwill-homeap	802.11a	171.70.35.135		Cisco-.1x	Alert	Unclassified	No

251891

Rogue AP Count Summary

This report displays a summarized count of all the rogue access points on your network.

Click **Rogue AP Count Summary** from the Report Launch Pad to open the Rogue AP Count Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Rogue AP Count Summary Reports page. See the "Configuring a Rogue AP Count Summary Report" section on page 14-185 and the "Rogue AP Count Summary Report Results" section on page 14-186 for more information.

Note You cannot upgrade the Rogue AP Count Summary reports to the NCS Release 1.0 and later.

Configuring a Rogue AP Count Summary Report

This section describes how to configure a Rogue AP Count Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.

  Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Classification Type—Choose **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to be displayed in the report results.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

  Note The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information about customizing report results.

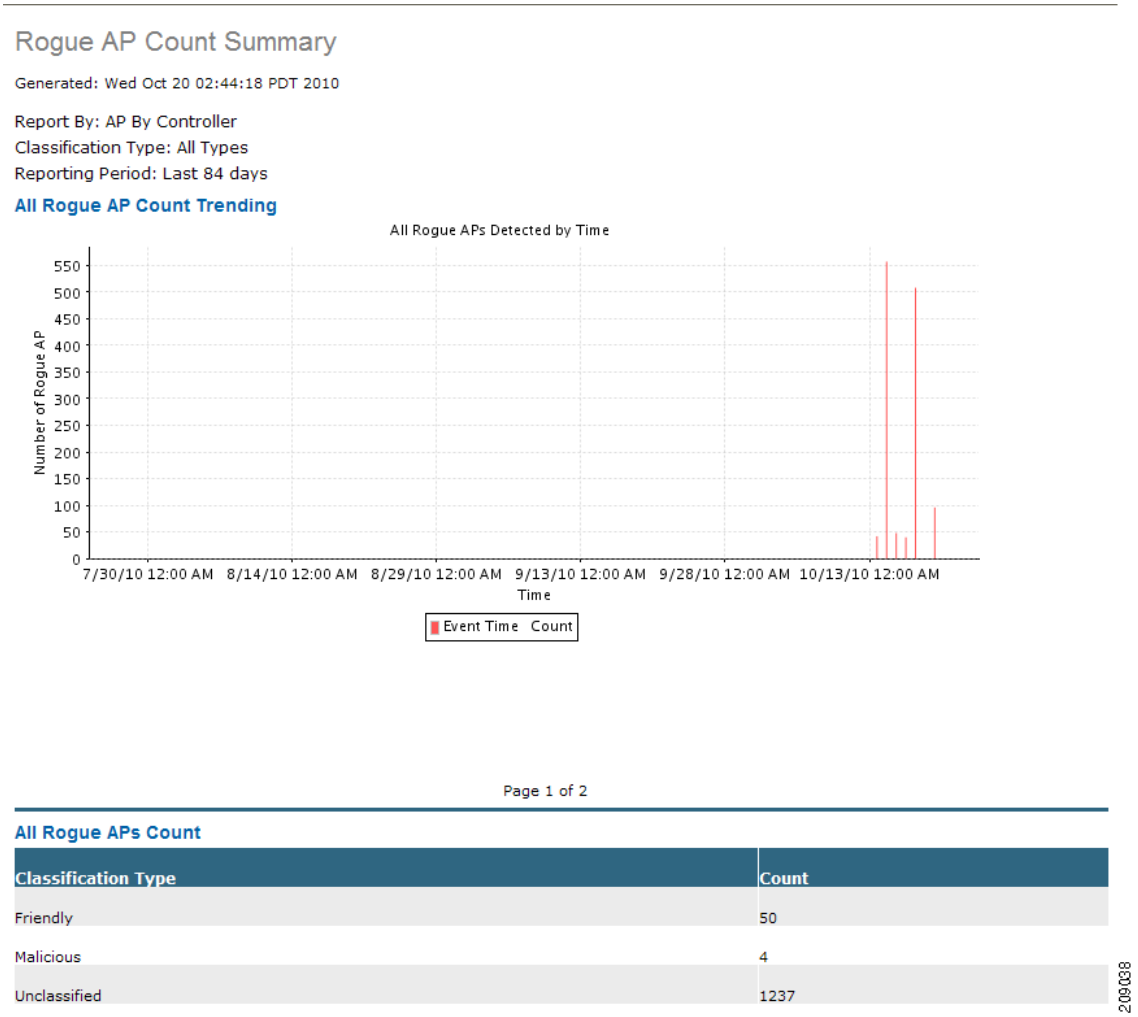
Note Data fields that appear in blue font cannot be removed from the list of fields to be included.

Rogue AP Count Summary Report Results

The following are potential results for a New Rogue AP Count Summary report, depending on how the report is customized (see Figure 14-55):

- All Rogue AP Count Trending graph
- All Rogue AP Count based on classification type

Figure 14-55 Rogue AP Count Summary Report



Rogue Access Point Events

This report displays all rogue access point events received by the NCS and based on the event time.

Any rogue-related trap received by the NCS is logged as a rogue event in the NCS. A new rogue access point event is created by the NCS based on polled data when there is a newly detected rogue access point. In addition, an event is also created by the NCS when the user changes the state and classification of the rogue access point through the NCS user interface.

Note One rogue can have multiple events. This report is based on the timestamp of the event.

Click **Rogue AP Events** from the Report Launch Pad to open the Rogue AP Events Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Rogue AP Events Reports page. See the "Configuring a Rogue Access Point Events Report" section on page 14-188 and the "Rogue AP Events Report Results" section on page 14-189 for more information.

Configuring a Rogue Access Point Events Report

Settings

The following settings can be configured for a Rogue Access Point Events report:

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report by
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria page, or click **Edit** to choose a specific device.

Note From the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Classification Type—Choose **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to display in the report results.
- Reporting Period
  - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
  - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Creating a Custom Report

The Create Custom Report page allows you to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

Command Buttons

Once all report parameters have been set, select from the following:

- Save—Click to save this report setup without immediately running the report. The report runs automatically at the scheduled time.
- Save and Run—Click to save this report setup and to immediately run the report.
- Run—Click to run the report without saving the report setup.
- Save and Export—Click to save the report and export the results to either CSV or PDF format.
- Save and Email—Click to save the report and e-mail the results.
- Export Now—Click to export the report results. The supported export formats is PDF and CSV.
- Cancel—Click to return to the previous page without running nor saving this report.

Note See the "Creating and Running a New Report" section on page 14-6 for additional information on running or scheduling a report.

Rogue AP Events Report Results

The following are potential results for a Rogue AP Events report, depending on how the report is customized:

- Last Seen Time (mandatory column)
- Rogue MAC Address (mandatory column)
- Detecting AP Name (mandatory column)
- Radio Type—802.11a/n or 802.11b/g/n.
- Controller IP Address—The IP address of the controller on which the rogue is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the rogue access point was detected.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state relative to the network or port. Rogue access point radios appear as "Alert" when first scanned by the port, or as "Pending" when operating system identification is still underway.
- Channel Number—The channel number of the rogue access point.
- RSSI (dBm)—The Received Signal Strength Indicator in dBm.
- SNR—The signal-to-noise ratio.
- Classification Type—The type of rogue access point (malicious, friendly, or unclassified).

Rogue APs

The NCS gets updates about rogues from controllers by using traps or by polling. The Last Seen Time is updated anytime a trap for the rogue is received or rogue was seen during the last polling cycles of the NCS.

This report displays all rogues detected by the access points in your network based on the "last seen time" of the rogue access points and the selected filtering criteria. It orders rogue access points based on the time they were last heard.

Note The report includes rogue access point alarms with clear severity.

Click **Rogue APs** from the Report Launch Pad to open the Rogue APs Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Rogue APs Reports page. See the "Configuring a Rogue APs Report" section on page 14-190 and the "Rogue APs Report Results" section on page 14-191 for more information.

Note You cannot upgrade the Rogue APs reports to the NCS Release 1.0 and later.

Configuring a Rogue APs Report

This section describes how to configure a Rogue APs report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Report By
  - AP by Controller—Choose **All Controllers > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Floor Area—Choose **All Campuses > All Buildings > All Floors > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.
  - AP by Outdoor Area—Choose **All Campuses > All Outdoor Areas > All Access Points** from the Report Criteria drop-down list or click **Edit** to choose a specific device.

  Note From the Filter Criteria drop-down list, choose the appropriate filter criteria.

- Classification Type—Choose **All Types**, **Malicious**, **Friendly**, or **Unclassified** to determine the type of rogue access point to display in the report results.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

  Note The times are shown in the local time of the NCS server.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Customize Report Form

Click **Customize** to open the Create Custom Report form, which you can use to customize the report results. See the "Creating and Running a New Report" section on page 14-6 for more information on customizing report results.

Note Fields that appear in blue font in the Data fields to include list are mandatory fields for this subreport.

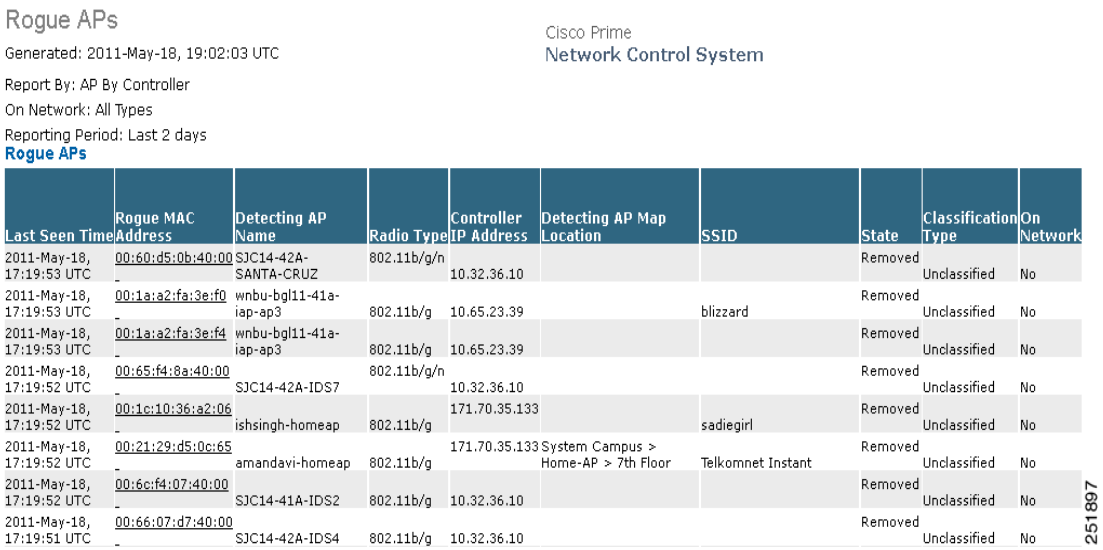
Rogue APs Report Results

The following are potential results for a Rogue APs report, depending on how the report is customized (see Figure 14-56):

Note The results for this report are sorted by "Last Seen" time.

- Last Seen Time—The date and time the rogue access point was last detected.
- Rogue MAC Address—The MAC address of the rogue access point. Click an item under MAC Address to view Rogue AP details.
- Detecting AP Name—The access point that last detected the rogue, when a rogue is detected by multiple access points on one controller. This last detected access point name comes from the controller which supports maximum RSSI.
- Radio Type—802.11a or 802.11b/g.
- Controller IP Address—The IP address of the controller on which the rogue is located.
- Map Location—The building, floor area, or outdoor area (as applicable) where the rogue access point is located.
- SSID—The user-defined Service Set Identifier name.
- State—The radio state relative to the network or port. Rogue access point radios appear as "Alert" when first scanned by the port, or as "Pending" when operating system identification is still underway.
- Channel Number—The channel number of the rogue access point.
- RSSI (dBm)—The maximum Received Signal Strength Indicator ever reported by any controller for this rogue.
- Classification Type—The type of rogue access point (malicious, friendly, or unclassified).
- Switch Port Trace Status—Indicates whether or not the switch port was traced.
- Switch Port Trace Summary—Provides a summary of the switch port trace or remains blank if no switch port was traced.
- On Network—Indicates whether the access point is on the network or not.

Figure 14-56 Rogues APs Report



Rogue APs

Generated: 2011-May-18, 19:02:03 UTC

Report By: AP By Controller

On Network: All Types

Reporting Period: Last 2 days

Cisco Prime
Network Control System

Rogue APs

Last Seen Time	Rogue MAC Address	Detecting AP Name	Radio Type	Controller IP Address	Detecting AP Map Location	SSID	State	Classification Type	On Network
2011-May-18, 17:19:53 UTC	00:60:d5:0b:40:00	SJC14-42A-SANTA-CRUZ	802.11b/g/n	10.32.36.10			Removed	Unclassified	No
2011-May-18, 17:19:53 UTC	00:1a:a2:fa:3e:f0	wnbu-bgl11-41a-iap-ap3	802.11b/g	10.65.23.39		blizzard	Removed	Unclassified	No
2011-May-18, 17:19:53 UTC	00:1a:a2:fa:3e:f4	wnbu-bgl11-41a-iap-ap3	802.11b/g	10.65.23.39			Removed	Unclassified	No
2011-May-18, 17:19:52 UTC	00:65:f4:8a:40:00	SJC14-42A-IDS7	802.11b/g/n	10.32.36.10			Removed	Unclassified	No
2011-May-18, 17:19:52 UTC	00:1c:10:36:a2:06	ishsingh-homeap	802.11b/g	171.70.35.133		sadiegirl	Removed	Unclassified	No
2011-May-18, 17:19:52 UTC	00:21:29:d5:0c:65	amandavi-homeap	802.11b/g	171.70.35.133	System Campus > Home-AP > 7th Floor	Telkomnet Instant	Removed	Unclassified	No
2011-May-18, 17:19:52 UTC	00:6c:f4:07:40:00	SJC14-41A-IDS2	802.11b/g	10.32.36.10			Removed	Unclassified	No
2011-May-18, 17:19:51 UTC	00:66:07:d7:40:00	SJC14-42A-IDS4	802.11b/g	10.32.36.10			Removed	Unclassified	No

251897

Security Alarm Trending Summary

This report displays a summary of trends of security alarms over a period of time.

Click **Security Alarm Trending Summary** from the Report Launch Pad to open the Security Alarm Trending Summary Reports page. From this page, you can enable, disable, delete, or run currently saved report templates. See the "Managing Current Reports" section on page 14-14 for more information.

To create a new report, click **New** from the Report Launch Pad or from the Security Summary Reports page. See the "Configuring a Security Alarm Trending Summary Report" section on page 14-192 and the "Security Alarm Trending Summary Report Results" section on page 14-193 for more information.

Note You cannot upgrade the Security Alarm Trending Summary reports to the NCS Release 1.0 and later.

Configuring a Security Alarm Trending Summary Report

This section describes how to configure a Security Alarm Trending Summary report.

Settings

- Report Title—If you plan to use this as a saved report template, enter a report name.
- Reporting Period—Specify the time period for which the report needs to be generated. You can select from a list of choices defined such as Last 1 hour, Last 6 hours, and so on, or specify a custom period by selecting the From and To date and time.

Note The times are shown in the local time of the NCS server.

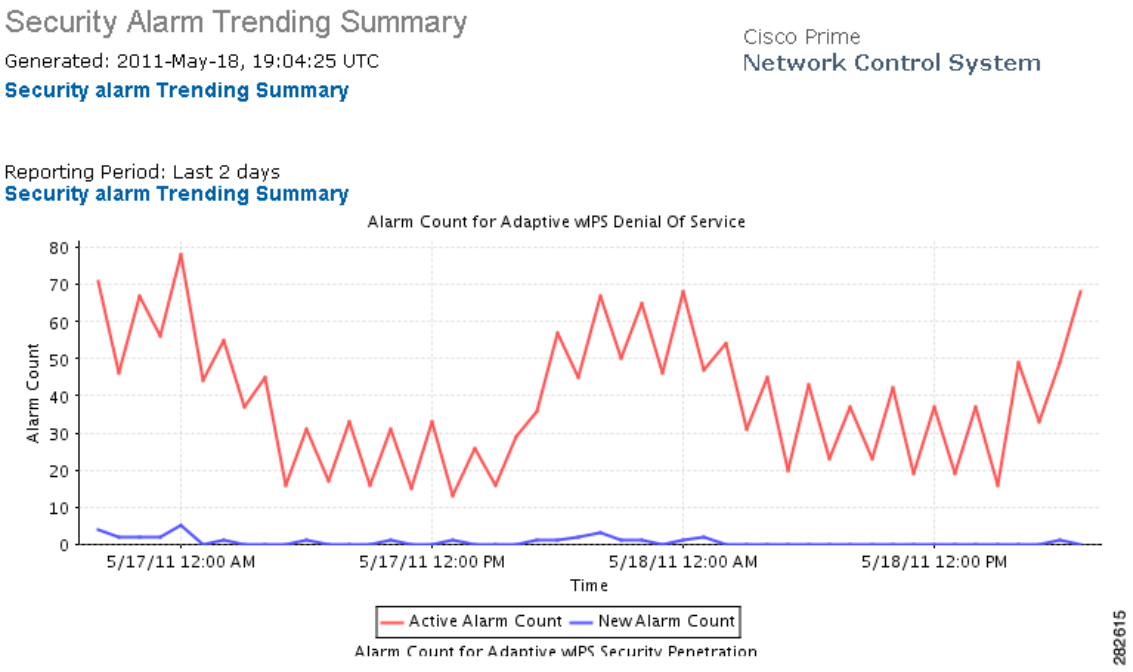
Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the "Creating and Running a New Report" section on page 14-6 for more information on scheduling a report.

Security Alarm Trending Summary Report Results

The following are potential results for a Security Alarm Trending Summary report, depending on how the report is customized (see Figure 14-57):

Figure 14-57 Security Alarm Trending Summary Report



CHAPTER 15

Performing Administrative Tasks

The Administration enables you to schedule tasks, administer accounts, and configure local and external authentication and authorization. Also, set logging options, configure mail servers, and data management related to configuring the data retain periods. Information is available about the types of NCS licenses and how to install a license.

This chapter describes the Cisco NCS administrative tasks. It contains the following sections:

Performing Background Tasks

You can use the NCS Background Tasks page to schedule and monitor data collection tasks and other background tasks.

This section contains the following topics:

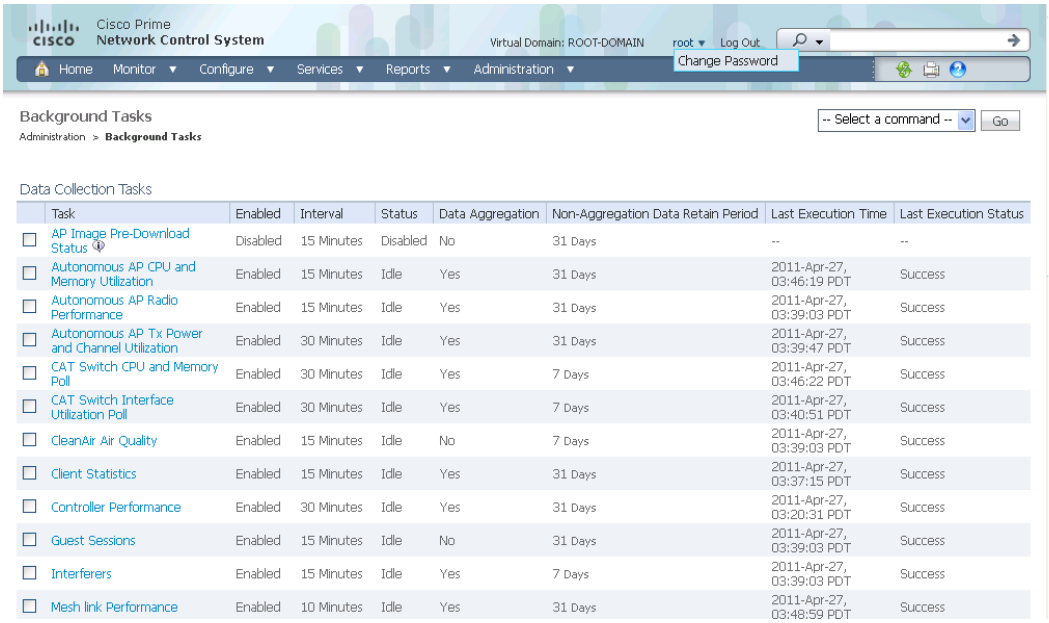
For more information on data collection and other background tasks, see the "Data Collection Tasks" section on page 15-5 and "Other Background Tasks" section on page 15-32.

About Background Tasks

A background task is a scheduled program running in the background with no visible pages or other user interfaces. In NCS background tasks can be anything from data collection to taking backups of the configurations.

Note Choose **Administration > Background Tasks** to view several scheduled tasks. The Background Tasks page appears (see Figure 15-1).

Figure 15-1 Background Tasks Page



You can view the administrative and operating status, task interval, and time of day in which the task occurs. To execute a particular task, select the check box of the desired task and choose **Execute Now** from the Select a command drop-down list. The task is executed based on what you have configured for the specific task.

The tasks are listed in tables with the following columns:

- Check box—Select to choose the desired task. Chosen tasks are targets for operations initiated from the Select a command drop-down list including the following:
  - Execute Now—Run all of the data sets with a selected check box.
  - Enable Collection—Enable the data set to run at its scheduled interval.
  - Disable Collection—Prevent the data set from running at its scheduled interval.
- Task—Task name that serves as a link to a configuration page. Click a task name to go to that task configuration page.
- Enabled—Indicates that the task is enabled or disabled.
- Interval—Time period between executions of task.
- Status—Indicates that the task is idle, disabled, or executing.
- Data Aggregation (Data Collections only)—If set to Yes, the data set is aggregate data.

- Non-Aggregation Data Retain Period (Days) (Data Collections only)—The number of days that non-aggregated data is retained.

Note See the "NCS Historical Data" section on page 15-60 for more information on aggregated and non-aggregated data in NCS.

- Last Execution Time—The date and time the task was executed.
- Last Execution Status—Indicates that the task executed was a success, failure, or a partial success.

This page enables you to view the status of scheduled NCS tasks. Scheduled tasks are divided into two types: for more information, see the "Data Collection Tasks" section on page 15-5 and the "Other Background Tasks" section on page 15-32.

Performing a Data Collection Task

Data collection tasks are data-set tasks that collect and organize information that might be useful for creating reports.

Note All tasks related to collecting data or any other background task are handled in a similar manner.

Step 1 Choose **Administration > Background Tasks** to display the Background Tasks page (see Figure 15-1). This page displays the following information:

- Enabled—Whether the tasks have been enabled or disabled.
- Interval—Indicates the time period (in minutes) between task executions. You can set the interval from the data collection configuration page for the task.
- Status—The present state of the task.
- Data Aggregation (Data Collection Tasks only)—If set to Yes, the data set combines data.
- Non-Aggregation Data Retain Period (Days) (Data Collection Tasks only)—The number of days that the non-aggregated data is retained. You can set the retention period from the data collection configuration page of the task.
- Last Execution Time—The time and date when the task was last run.
- Last Execution Status—The status after the last task was run.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**.

- Enable the task.

  Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task changes from dimmed to available after enabling is complete.

- Disable the task.

  Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task is dimmed after the disabling is complete.

- View details of a task.

  Click a URL in the Data Collection Tasks or Other Background Tasks column to view a specific task. The details on that task appear. Data collections are data-set tasks that collect and organize a specific type of information useful for creating reports. For more information on the various Data Collection Tasks, see "Data Collection Tasks" section on page 15-5.

To access the configuration page of a data set, select the name of the data set in the Data Collection page. Each data set configuration page displays a table of the executions of the data set. The table has following columns:

- Executed task information includes the following:
  - Last Execution Start Time—Indicates the date and time that the data-set task began running.
  - End Time—Indicates the date and time that the data-set task stopped running.
  - Elapsed Time (secs)—Indicates the amount of time (in seconds) it took to complete the task.
  - Result—Indicates the success or failure of the task.
  - Additional Information—Provides any additional information regarding a specific task.

Each data set configuration page contains the following parameters and information in the Collection Set Details group box:

- Description—Provides a brief display only description of the data set.
- Data Aggregation—Indicates whether or not data collected by the data set is aggregated.
- Used By Report(s)—Displays names of the reports that use the data set.
  - CleanAir Air Quality—This data set is used for Worst Air Quality APs and Air Quality versus Time reports.
  - Interferers—This data set us used for Worst Interferers reports.
- Collection Status—Select the **Enabled** check box to enable data collection.

Interval (min.)—Enter the time (in minutes) for the data set execution interval. The valid value is 1 to 120 minutes.

Each data set configuration page contains the following parameters in the Data Management group box:

- Non-Aggregation Data Retain Period (Days)—Enter the number of days to retain non-aggregated data collected by the data set. The valid value is 1 to 31 days.
- Retain Aggregation Raw Data—Select the **Enable** check box to enable the retention of aggregated raw data.

Note The Aggregation Raw Data Retain Period setting is for polled raw data. To configure the retention period for aggregated trend data, choose **Administration > Settings**, then choose **Data Management** from the left sidebar menu.

Note See the "Configuring Auto Provisioning for Controllers" section on page 8-230 for more information on aggregated and non-aggregated data.

Note For this example, performing an NCS server backup was selected as the task. The information entered in the fields for each page vary based on the task you choose.

Step 3 Select the **Enabled** check box.

Step 4 Select the **Report History Backup** check box.

Step 5 In the Max Backups to Keep text box, enter the maximum number of backup files to save on the server.

Range: 7 to 50

Default: 7

Note To prevent the NCS platform from running out of disk space, the server automatically deletes old backup files when the number of files exceeds the value entered for this text box.

Step 6 In the Interval (Days) text box, enter the number of days between each backup. For example, 1 = a daily backup, 2 = a backup every other day, 7 = a weekly backup, and so on.

Range: 1 to 360

Default: 7

Step 7 In the Time of Day text box, enter the backup start time. It must be in this format: *hh*:*mm AM/PM* (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

Note Backing up a large database affects the performance of the NCS server. Therefore, we recommend that you schedule backups to run when the NCS server is idle (for example, in the middle of the night).

Step 8 Click **Submit** to save your settings. The backup file is saved as a .zip file in the ftp-install-dir/ftp-server/root/NCSBackup directory using this format: *dd-mmm-yy_ hh-mm-ss*.zip (for example, 11-Nov-05_10-30-00.zip).

Data Collection Tasks

Table 15-1 lists and describes the various data collection tasks in the NCS.

Table 15-1 Data Collection Tasks

Task Name	Task Status	Default Schedule	Description
AP Image Pre-Download Status	Disabled	15 minutes	This task is used to see the Image Predownload status of the associated APs in the controllers. To see the status of the access points, the Pre-download software to APs check box should be selected while downloading software to the controller.
Autonomous AP CPU and Memory Utilization	Enabled	15 minutes	This task is used to collect information about memory and CPU utilization of autonomous APs.
Autonomous AP Inventory	Enabled	180 minutes	This task is used to collect the inventory information for autonomous APs.

Table 15-1 Data Collection Tasks (continued)

Task Name	Task Status	Default Schedule	Description
Autonomous AP Radio Performance	Enabled	15 minutes	This task is used to collect information about radio performance information as well as radio up or down status for autonomous APs.
Autonomous AP Tx Power and Channel Utilization	Enabled	30 minutes	This task is used to collect information about radio performance of autonomous APs.
CAT Switch CPU and Memory Poll	Enabled	30 minutes	This task is used to collect information about CAT switch CPU and memory p oll.
CAT Switch Interface Utilization Poll	Enabled	30 minutes	This task is used to collect information about CAT switch interface utilization poll.
CleanAir Air Quality	Enabled	15 minutes	This task is used to collect information about CleanAir air quality.
Client Statistics	Enabled	15 minutes	This task helps you to get the statistical information for the autonomous and lightweight clients.
Controller Performance	Enabled	30 minutes	This task is used to collect performance information for controllers.
Guest Sessions	Enabled	15 minutes	This task is used to collect information about the guest sessions.
Interferers	Enabled	15 minutes	This task is used to collect information about the interferers.
Media Stream Clients	Enabled	15 minutes	This task is used to collect information about media stream for clients.
Mesh link Performance	Enabled	10 minutes	This task is used to collect information about the performance of Mesh links.
Mesh Link Status	Enabled	5 minutes	This task is used to collect status of the Mesh links.
Mobility Service Performance	Enabled	15 minutes	This task is used to collect information about the performance of mobility service engines.
Radio Performance	Enabled	15 minutes	This task is used to collect statistics from wireless radios.
Rogue AP	Enabled	120 minutes	This task is used to collect information about the rogue access points.
Traffic Stream Metrics	Enabled	8 minutes	This task helps you to get traffic stream metrics for the clients.
CCX Client Statistics	Disabled	60 minutes	This task is used to collect the Dot11 and security statistics for CCX Version 5 and Version 6 clients.
Wired Switch Inventory	Enabled	Daily at midnight	This task is used to collect inventory information for wired switches.
Wireless Controller Inventory	Disabled	Daily at midnight	This task is used to collect inventory information for wireless controllers.

Performing Other Background Tasks

You can also perform other background tasks using the NCS Administration.

This section contains the procedures for the other NCS background tasks and contains the following topics:

For more information on the other background tasks, see the "Other Background Tasks" section on page 15-32.

Viewing Appliance Status

To view the appliance status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Appliance Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

or

- Enable the task.

  Select the **Appliance Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Appliance Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the **Appliance Status** link in the Background Tasks column. The Task > Appliance Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

The Appliance Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time (in seconds) of the task.
  - Result—Success or error.
  - Message—Text message regarding this task.

Step 5 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Interval—Indicates the frequency (in minutes) of the task.

Step 6 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Autonomous AP Client Status

To view the Autonomous AP Client Status page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Autonomous AP Client Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Autonomous AP Client Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Autonomous AP Client Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the **Autonomous AP Client Status** link in the Background Tasks column. The Task > Autonomous AP Client Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

The Autonomous AP Client Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time (in seconds) of the task.
  - Result—Success or error.
  - Message—Text message regarding this task.

Step 5 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Interval—Indicates the frequency (in minutes) of the task.

Step 6 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Autonomous AP Operational Status

To view the Autonomous AP Operational Status page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Autonomous AP Operational Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Autonomous AP Operational Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Autonomous AP Operational Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the **Autonomous AP Operational Status** link in the Background Tasks column. The Task > Autonomous AP Operational Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

The Appliance Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time (in seconds) of the task.
  - Result—Success or error.
  - Message—Text message regarding this task.

Step 5 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Interval—Indicates the frequency (in minutes) of the task.

Step 6 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing a Configuration Sync

To perform a configuration sync, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Configuration Sync** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Configuration Sync** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

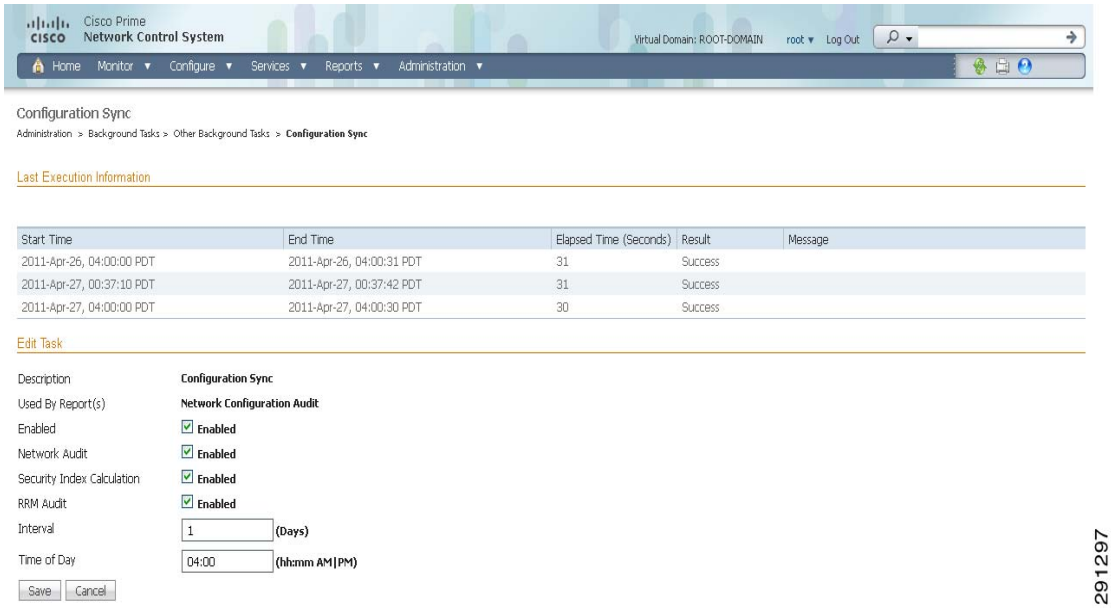
  or

- Disable the task.

  Select the **Configuration Sync** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the **Configuration Sync** link in the Background Tasks column. The Task > Configuration Sync page appears (see Figure 15-2).

Figure 15-2 Task > Configuration Sync



Step 4 Click the background task in the Task column to open the task details page.

The Configuration Sync page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time (in seconds) of the task.
  - Result—Success, warning, or error.
  - Message—Text message regarding this task.

Note If the Result is a Warning and the Message appears as Failed, the device is unreachable.

Step 5 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Used By Report(s)—Indicates the NCS reports that use these task results.
- Enabled—Select the check box to enable this task.
- Network Audit—Select the check box to enable the secondary network audit.
- Security Index Calculation—Select the check box to enable security index calculation. The Security Index is available in the Monitor > Security page.
- RRM Audit—Select the check box to enable an RRM audit.

Note The controller audit finds the discrepancies between the values in the NCS database with the device.

Note To query the SNMP values from the device, you can use the https://<NCS-IP>/webacs/manObjDiagQueryAction.do URL in the NCS.

Note The Network Audit audits all controllers in the network, and also runs the RRM audit and Security audit. These options are selectable from the **Administration > Background Tasks > Other Background Tasks > Configuration Sync** page.

- Time of Day (hh:mm AM|PM)—Indicate the time of day (AM or PM) for the execution of this task.

Note Time of Day (hh:mm AM|PM) must be in this format: hh:mm AM/PM (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

Step 6 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Lightweight Client Status

Choose **Administration > Background Tasks**, then click **Lightweight Client Status** to access this page.

This page enables you to view the history and current status of lightweight client status polling backups.

In the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The Lightweight Client Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 3 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Controller Configuration Backup Status

Choose **Administration > Background Tasks**, then click **Controller Configuration Backup** to access this page.

This page enables you to view the history and current status of Cisco WLAN Solution configuration backups.

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The Controller Configuration Backup page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.
- Time of Day (hh:mm AM|PM)

Note Time of Day (hh:mm AM|PM) must be in this format: hh:mm AM/PM (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

- TFTP Server or FTP Server—Select either of the following:
  - TFTP Server—If you select TFTP Server, choose the server or **Default Server** from the drop-down list.
  - FTP Server—If you select FTP Server, choose the server or **Default Server** from the drop-down list, enter the FTP Username, FTP Password and FTP port information in the respective text box.

Note TFTP must be enabled in Administration > Settings > Server Settings for 'Default Server' options. For more information, see the "Configuring Server Settings" section on page 15-71.

Note The Server drop-down list is populated with the server names only if you add FTP or TFTP servers in the NCS. To add an FTP or TFTP server, see the "Configuring TFTP or FTP Servers" section on page 8-247.

Step 3 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Controller Operational Status

Device status polls controller reachability and WiSM peer information.

Choose **Administration > Background Tasks**, then click **Controller Operational Status** to access this page.

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable Controller Operational Status task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the **Controller Operational Status** check box to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the **Controller Operational Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the **Controller Operational Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the Controller Operational Status task, follow these steps:

Step 1 Click the Controller Operational Status background task in the Task column to open the task details page.

The Controller Operational Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

  Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in minutes) of the task.

Step 3 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Data Cleanup Status

Choose **Administration > Background Tasks**, then click **Database Cleanup** to access this page.

This page enables you to view the history and current status of Cisco WLAN Solution database cleanups.

To modify this task, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Click the background task in the Task column to open the task details page.

The Data Cleanup page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 3 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Time of Day (hh:mm AM|PM)

Note Time of Day (hh:mm AM|PM) must be in this format: hh:mm AM/PM (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

Step 4 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing Device Data Collection

To perform a device data collection, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Device Data Collection** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Device Data Collection** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Device Data Collection** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the **Device Data Collection** link in the Background Tasks column. The Task > Device Data Collector page appears.

Step 4 Click the background task in the Task column to open the task details page.

The Device Data Collector page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time (in seconds) of the task.
  - Result—Success or error.
  - Message—Text message regarding this task.

Step 5 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Controller IP address—The IP address of the controller to collect data from.
- CLI Commands—Enter the command-line interface commands separated by comma, which you would want to run on the specified controller.
- Clean Start—Select or unselect this check box to enable or disable a clean start before data collection.
- Repeat—Enter the number of times you would want the data collection to happen.
- Interval—Enter the interval, in days, that you would want the data collection to happen. The valid range is 1 to 360 days.

Step 6 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing Guest Accounts Sync

Choose **Administration > Background Tasks**, then click **Guest Accounts Sync** to access this page.

This page enables you to view the history and current status of Guest Accounts Synchronization tasks.

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The Guest Accounts Synchronization page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

  Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.
- Time of Day (hh:mm AM|PM)

  Note Time of Day (hh:mm AM|PM) must be in this format: hh:mm AM/PM (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

Step 3 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Identity Services Engine Status

To update the identity services engine status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

Select the **Identity Services Engine Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

or

- Enable the task.

  Select the **Identity Services Engine Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Identity Services Engine Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the Identity Services Engine Status task, click the **Identity Services Engine Status** link in the Background Tasks column. The Identity Services Engine Status page appears.

Step 4 Click the Identity Services Engine Status background task in the Task column to open the task details page.

Step 5 The Identity Services Engine Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

  Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Updating License Status

To update the license status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

Select the **License Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

or

- Enable the task.

  Select the **License Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

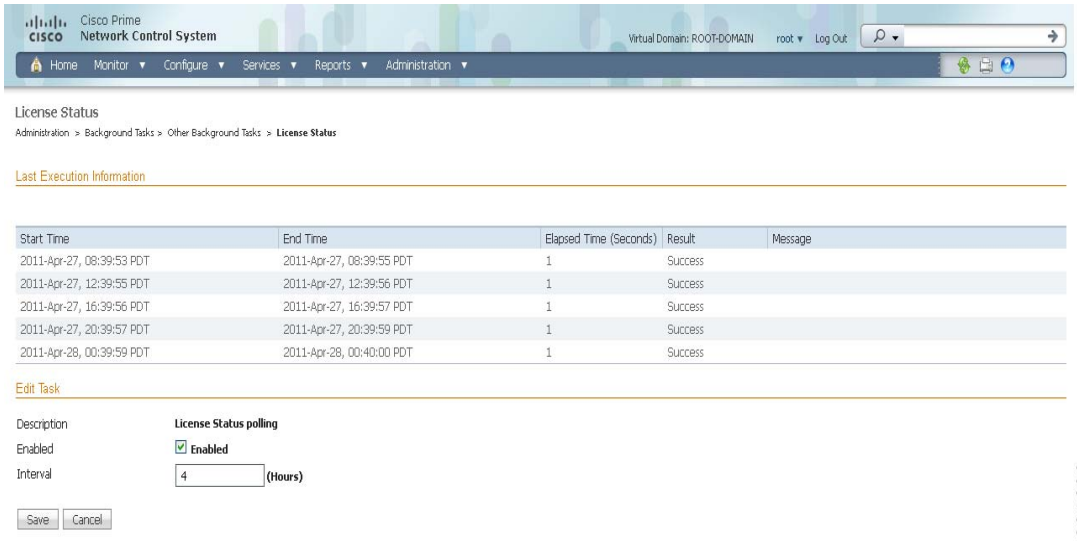
  or

- Disable the task.

  Select the **License Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the controller license reset task, click the **License Status** link in the Background Tasks column. The License Status page appears (see Figure 15-3).

Figure 15-3 License Status Page



This page shows when the latest license resynchronizations occurred. By default, it runs every 4 hours. From this page, you can disable this task or change the interval.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The License Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.

- Enabled—Select this check box to enable the task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Lightweight AP Operational Status

To view the Lightweight AP Operational status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Lightweight AP Operational Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Lightweight AP Operational Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Lightweight AP Operational Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the controller license reset task, click the **Lightweight AP Operational Status** link in the Background Tasks column. The License Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The Lightweight AP Operational Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable the task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Lightweight AP Client Status

To view the Lightweight AP Client status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Lightweight AP Client Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Lightweight AP Client Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Lightweight AP Client Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the controller license reset task, click the **Lightweight AP Client Status** link in the Background Tasks column. The License Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The Lightweight AP Client Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing Location Appliance Backup

Choose **Administration > Background Tasks**, then click **Location Appliance Backup** to access this page.

This page enables you to schedule a backup of the mobility services engine database.

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The Mobility Service Backup page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Max backups to keep—Enter the maximum number of location backups to be kept on the backup server.
- Interval (days)—Enter the frequency of backup.
- Time of the Day (hh:mm AM/PM)—Enter the time at which the backup starts on the scheduled day.

Note Time of Day (hh:mm AM|PM) must be in this format: hh:mm AM/PM (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

- When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Location Appliance Status

Choose **Administration > Background Tasks**, then click **Location Appliance Status** to access this page.

This page displays the status of the mobility services engine.

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The Mobility Service Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval (days)—Enter the frequency of backup.

Step 3 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing Location Appliance Synchronization

Choose **Administration > Background Tasks**, then click **Location Appliance Synchronization** to access this page.

This page enables you to synchronize mobility services engine(s).

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The Mobility Service Synchronization page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Out of Sync Alerts—When enabled, this generates minor alarms when location server is not synchronized with the NCS changes that you have made.
- Auto Synchronization—Use this setting to enable auto synchronization of the location server. This ensures that when you make changes to the NCS, the location server auto synchronizes with the changes.
- Interval (minutes)—Specify the auto synchronization interval.

Step 3 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing NCS Server Backup

Choose **Administration > Background Tasks**, then click **NCS Server Backup** to access this page.

This page enables you to schedule a backup of the NCS server.

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The NCS Server Backup page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Report History Backup—Select the check box to enable the NCS to back up report histories.
- Max Backups to Keep—Enter the maximum number of NCS server backups to be kept on the backup server.
- Backup Repository—Select an existing backup repository or click **Create** to create a new backup repository.
- Interval (days)—Enter a value between 1 and 360. The NCS server data is backed up every *n* days, where *n* is the value that you have specified in this field.
- Time of the Day (hh:mm AM/PM)—Enter the time at which the backup starts on the scheduled day.

Note Time of Day (hh:mm AM|PM) must be in this format: hh:mm AM/PM (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

- When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing OSS Server Status

To view the OSS Server status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **OSS Server Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **OSS Server Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **OSS Server Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the controller license reset task, click the **OSS Server Status** link in the Background Tasks column. The OSS Server Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The OSS Server Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

  Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing the Switch NMSP and Location Status

You can view the Switch NMSP and Location Status using the Switch NMSP and Location Status option under Cisco NCS Administration.

To view the Switch NMSP and Location Status, follow these steps:

Step 1 Choose **NCS > Administration > Background Tasks**.

Step 2 From the Other Background Tasks table, click the **Switch NMSP and Location Status** link.

The Switch NMSP and Location Status page appears.

The Switch NMSP and Location Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.

- Result—Success or error.
- Message—Text message regarding the task execution.

Step 3 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval (hours)—Enter the frequency of backup.

Step 4 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Switch Operational Status

To view the Switch Operational status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Switch Operational Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Switch Operational Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Switch Operational Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to avaialble in the Enabled column after the disabling is complete.

Step 3 To modify the Switch Operational Status task, click the **Switch Operational Status** link in the Background Tasks column. The Switch Operational Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The Switch Operational Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

  Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing wIPS Alarm Synchronization

To perform wIPS Alarm Synchronization, follow these steps :

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **wIPS Alarm Sync** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **wIPS Alarm Sync** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **wIPS Alarm Sync** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the wIPS Alarm Sync task, click the **wIPS Alarm Sync** link in the Background Tasks column. The wIPS Alarm Sync page appears.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The wIPS Alarm Sync page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Wired Client Status

To view the Wired Client status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Wired Client Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Wired Client Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Wired Client Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the Wired Client Status task, click the **Wired Client Status** link in the Background Tasks column. The Wired Client Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The Wired Client Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Enter the interval, in hours, that you want the wired client status polling to happen. The valid range is 1 to 8640 hours.
- Major Polling—Specify two time periods at which you want the major pollings to happen. Valid format: hh:mm AM|PM. Example: 12:49 AM.

  For wired clients, the NCS polls managed switches at regular interval to discover new clients or changes to the existing clients. To find this, the NCS caches the last change time of the interface. In the next poll, it checks the new value of the change time of the interface with the cached value to determine whether there is any change on any interface. Then polling happens only for the interfaces where there is a change. If there is no change on an interface between the polling, no polling happens for that interface. When polling happens during major polling schedule, a complete polling is done irrespective of whether there is a change on the interface or not. The reason for having major and minor polling is because, polling the switches for wired clients on all interfaces is expensive and resource-intensive for the NCS and switches. So then, the major polling happens only twice a day.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Other Background Tasks

Table 15-2 describes the other background tasks that are available in the NCS:

Table 15-2 Other Background Tasks

Task Name	Default Schedule	Description	Editable Options
Appliance Status	5 minutes	This task is used to view the details of the appliance polling. This task populates the appliance polling details from **Administration > Appliance > Appliance Status** page. In addition, this background task populates information such as the performance and fault checking capabilities of the appliance.	Default—Enabled Interval—Valid interval - 1 - 10080 For more information, see the "Viewing Appliance Status" section on page 15-7.
Autonomous AP Client Status	5 minutes	This task helps you to discover the autonomous AP client from the network.	Default—Enabled. For more information, see the "Viewing Autonomous AP Client Status" section on page 15-8.
Autonomous AP Operational Status	5 minutes	This task helps you to view the autonomous AP operational status polling.	Default: Enabled Interval—Valid interval - 1 - 10080 For more information, see the "Viewing Autonomous AP Operational Status" section on page 15-9.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Configuration Sync	Daily at 4 am.	This task is used to view the configuration synchronization.	Enable—Select or unselect this check box to enable or disable configuration synchronization. Default: Enabled. Enable—Select or unselect this check box to enable or disable Network Audit. Default: Enabled. Enable—Select or unselect this check box to enable or disable Security Index calculation. Default: Enabled. Enable—Select or unselect this check box to enable or disable RRM audit. The default is Enabled. Interval—Enter the interval, in days, that you want the configuration synchronization to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the configuration synchronization to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. For more information, see the "Performing a Configuration Sync" section on page 15-10.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Controller Configuration Backup	Daily at 10 pm	This task is used to view the controller configuration backup activities.	Enable—Select or unselect this check box to enable or disable controller configuration backup. The default is Disabled. Interval—Enter the interval, in days, that you want the configuration synchronization to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the configuration synchronization to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. TFTP Server—Select the IP address of the server to which you want to back up the controller configuration. For more information, see the "Viewing Controller Configuration Backup Status" section on page 15-13.
Controller Operational Status	5 minutes	This task is used to schedule and view the controller operational status.	Enable—Select or unselect this check box to enable or disable Controller Configuration Backup. The default is enabled. Interval—Enter the interval, in days, that you want the configuration synchronization to happen. The valid range is 1 to 360 days. For more information, see the "Viewing Controller Operational Status" section on page 15-15.
Data Cleanup	Daily at 2 am.	This task is used to schedule a data cleanup	Time of Day—Enter the time of the day that you want the data cleanup to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. The default is Enabled. For more information, see the "Viewing Data Cleanup Status" section on page 15-16.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Device Data Collector	30 minutes	This task is used to schedule a data collection based on the specified command-line interface commands at a configured time interval.	Enabled—Select or unselect this check box to enable or disable data collection for a specified controller. The default is Disabled. Controller IP address—The IP address of the Controller to collect data from. CLI Commands—Enter the CLI commands, separated by commas, which you want to run on the specified controller. Clean Start—Select or unselect this check box to enable or disable a clean start before data collection. Repeat—Enter the number of times that you want the data collection to happen. Interval—Enter the interval, in days, that you want the data collection to happen. The valid range is 1 to 360 days. For more information, see the "Performing Device Data Collection" section on page 15-16.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Guest Accounts Sync	Daily at 1 am.	This task is used to schedule guest account polling and synchronization.	Enable—Select or unselect this check box to enable or disable guest account synchronization. The default is Enabled. Interval—Enter the interval, in days, that you want the guest account synchronization to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the guest account synchronization to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. For more information, see the "Performing Guest Accounts Sync" section on page 15-17.
Identity Services Engine Status	15 minutes	This task is used to schedule the Identity Services Engine polling.	Enable—Select or unselect this check box to enable or disable Identity Services Engine polling. The default is Enabled. Interval—Enter the interval, in days, that you want the Identity Services Engine polling to happen. The valid range is 1 to 360 days. For more information, see the "Viewing Identity Services Engine Status" section on page 15-19.
License Status	4 hours.	This task is used to schedule the license status polling.	Enable—Select or unselect this check box to enable or disable license status polling. The default is Enabled. Interval—Enter the interval, in days, that you want the license status polling to happen. The valid range is 1 to 360 days. For more information, see the "Updating License Status" section on page 15-20.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Lightweight AP Operational Status	5 minutes.	This task helps you to view the Lightweight AP operational status polling.	Enable—Select or unselect this check box to enable or disable Lightweight AP Operational Status polling. The default is Enabled. Interval—Enter the interval, in days, that you want the Lightweight AP Operational Status polling to happen. The valid rangeis 1 to 360 days. For more information, see the "Lightweight AP Operational Status" section on page 15-21.
Lightweight Client Status	5 minutes.	This task helps you to discover the Lightweight AP client from the network.	Enable—Select or unselect this check box to enable or disable Lightweight Client Status polling. The default is Enabled. Interval—Enter the interval, in days, that you want the Lightweight Client Status polling to happen. The valid range is 1 to 360 days. For more information, see the "Lightweight AP Client Status" section on page 15-22.
Mobility Service Backup	Every 7 days at 1 am.	This task is used to schedule mobility services backup polling.	Enable—Select or unselect this check box to enable or disable mobility service backup. The default is disabled. Interval—Enter the interval, in days, that you want the mobility services back up to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the mobility services back up to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. For more information, see the "Performing Location Appliance Backup" section on page 15-23.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Mobility Service Status	5 minutes.	This task is used to schedule mobility services status polling.	Enable—Select or unselect this check box to enable or disable mobility services status polling. The default is Enabled. Interval—Enter the interval, in days, that you want the mobility services status polling to happen. The valid range is 1 to 360 days. For more information, see the "Viewing Location Appliance Status" section on page 15-24.
Mobility Service Synchronization	60 minutes.	This task is used to schedule mobility services synchronization.	Out of Sync Alerts—Select this check box if you want to enable out of sync alerts. Smart Synchronization—Select this check box if you want to enable smart synchronization. The default is Enabled. Interval—Enter the interval, in minutes, that you want the mobility services synchronization to happen. The valid range is 1 to 10080 minutes. For more information, see the "Performing Location Appliance Synchronization" section on page 15-25.
NCS Server Backup	Every 7 days at 1 am.	This task is used to schedule the NCS server backup.	Enable—Select or unselect this check box to enable or disable NCS server backup. The default is Disabled. Interval—Enter the interval, in days, that you want the NCS server back up to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the NCS server back up to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. For more information, see the "Performing NCS Server Backup" section on page 15-26.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
OSS Server Status	5 minutes.	This task is used to schedule OSS server status polling.	Enable—Select or unselect this check box to enable or disable OSS Server polling. The default is Enabled. Interval—Enter the interval, in minutes, that you want the OSS server polling to happen. The valid range is 1 to 10080 minutes. For more information, see the "Viewing OSS Server Status" section on page 15-28.
Switch NMSP and Location Status	4 hours	This task is used to schedule the Switch NMSP and Civic Location Polling.	Enable—Select or unselect this check box to enable or disable Switch NMSP and Civic Location polling. The default is Enabled. Interval—Enter the interval, in minutes, that you want the Switch NMSP and Civic Location Polling to happen. The valid range is 1 to 10080 minutes. For more information, see the "Viewing the Switch NMSP and Location Status" section on page 15-29.
Switch Operational Status	5 minutes. Full poll is 15 minutes.	This task is used to schedule switch operational status polling.	Enable—Select or unselect this check box to enable or disable Switch NMSP and Civic Location polling. Interval—Enter the interval, in minutes, that you want the Switch NMSP and Civic Location Polling to happen. The valid range is 1 to 10080 minutes. Full operational status interval—Enter the interval, in minutes. The valid range is 1 to 1440 minutes. For more information, see the "Viewing Switch Operational Status" section on page 15-29.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
wIPS Alarm Sync	120 minutes.	This task is used to schedule wIPS alarm synchronization.	Enable—Select or unselect this check box to enable or disable wIPS alarm synchronization. The default is Enabled. Interval—Enter the interval, in minutes, that you want the wIPS alarm synchronization to happen. The valid range is 1 to 10080 minutes. For more information, see the "Performing wIPS Alarm Synchronization" section on page 15-30.
Wired Client Status	2 hours.	This task is used to schedule wired client status polling.	Enable—Select or unselect this check box to enable or disable wired client status polling. The default is Enabled. Interval—Enter the interval, in hours, that you want the wired client status polling to happen. The valid range is 1 to 8640 hours. Major Polling—Specify two time periods that you want the major pollings to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. For more information, see the "Wired Client Status" section on page 15-31.

Configuring a Virtual Domain

An NCS Virtual Domain consists of a set of NCS devices and/or maps and restricts the user view to information relevant to these managed objects.

Through a virtual domain, an administrator can ensure that users are only able to view the devices and maps for which they are responsible. In addition, because of the virtual domain filters, users are able to configure, view alarms, and generate reports for *only* their assigned part of the network.

Note The following elements can be partitioned in a virtual domain: maps, controllers, access points, templates, and config groups.
The following cannot be partitioned in a virtual domain (and are only available from the root partition: Google Earth Maps, Auto Provisioning, and Mobility Services).

The administrator specifies a set of allowed virtual domains for each user. Only one of these can be active for that user at login. The user can change the current virtual domain by choosing a different allowed virtual domain from the Virtual Domain drop-down list. All reports, alarms, and other functionality are now filtered by that virtual domain.

In the NCS Release 1.0 and later, you are required to add a virtual domain in ACS when exporting the task list to ACS. This might be the default ROOT-DOMAIN virtual domain. If you do not add a virtual domain to ACS then you are not permitted to log in. This applies regardless of whether you have a single or multiple domains.

Use the Administration > Virtual Domain page to create, edit, delete, import, or export virtual domains. Each virtual domain might contain a subset of the elements included with its parent virtual domain. You can assign additional maps, controllers, access points, and switches to the new virtual domain. See the "Managing a Virtual Domain" section on page 15-47 for more information on managing virtual domains.

The following buttons are available in the Virtual Domain page:

- New—Click to create a new virtual domain. See the "Creating a New Virtual Domain" section on page 15-46 for more information.
- Delete—Click to delete the selected virtual domain from the hierarchy.
- Import—Click to import a CSV file.
- Export—Click to configure custom attributes for the selected virtual domain. See the "Virtual Domain RADIUS and TACACS+ Attributes" section on page 15-49 for more information.

This section contains the following topics:

Understanding Virtual Domain Hierarchy

Virtual domains are organized hierarchically. Subsets of an existing virtual domain contain the network elements that are contained in the parent virtual domain.

Note The default or "ROOT-DOMAIN" domain includes all virtual domains.

Because network elements are managed hierarchically, some features and components such as report generation, searches, templates, config groups, and alarms are affected.

Note If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports. If you create a partition with only a few controllers, choose **Configure > Access Points**, and click an individual link in the AP Name column, the complete list of NCS-assigned controllers is displayed for primary, secondary, and tertiary controllers rather than the limited number specified in the partition.

Note If the configuration of a controller is modified by multiple virtual domains, complications might arise. To avoid this, manage each controller from only one virtual domain at a time.

This section describes the effects of partitioning and contains the following topics:

Reports

Reports only include components assigned to the current virtual domain. For example, if you create a virtual domain with only access points and no controllers assigned, all controllers are not displayed when you generate a controller inventory report.

If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports.

Note Reports are only visible in the current virtual domain. The parent virtual domain cannot view the reports from its subvirtual domain.

Client reports such as Client Count only include clients that belong to the current virtual domain.

Note If new clients are assigned to this partition by the administrator, the previous reports do not reflect these additions. Only new reports reflect the new clients.

Search

Search results only include components that are assigned to the virtual domain in which the search is performed. Search results do not display floor areas when the campus is not assigned to the virtual domain.

Note The saved searches are only visible in the current virtual domain. The parent virtual domain cannot view these search results.

Note The NCS does not partition network lists. If you search a controller by network list, all controllers are returned.

Note Search results do not display floor areas when the campus is not assigned to the virtual domain.

Alarms

When a component is added to a virtual domain, no previous alarms for that component are visible to that virtual domain. Only newly-generated alarms are visible. For example, when a new controller is added to a virtual domain, any alarms generated for that controller prior to its addition do not appear in the current virtual domain.

Alarms are not deleted from a virtual domain when the associated controllers or access points are deleted from the same virtual domain.

Note Alarm Email Notifications—Only the ROOT-DOMAIN virtual domain can enable Location Notifications, Location Servers, and NCS e-mail notification.

Templates

When you create or discover a template in a virtual domain, it is only available to that virtual domain unless it is applied to a controller. If it is applied to a controller and that controller is assigned to a subvirtual domain, the template stays with the controller in the new virtual domain.

Note If you create a subvirtual domain and then apply a template to both network elements in the virtual domain, the NCS might incorrectly reflect the number of partitions to which the template was applied.

Config Groups

Config groups in a virtual domain can also be viewed by the parent virtual domain. A parent virtual domain can modify config groups for a sub (child) virtual domain. For example, the parent virtual domain can add or delete controllers from a subvirtual domain.

Maps

You can only view the maps that your administrator assigned to your current virtual domain.

- When a campus is assigned to a virtual domain, all buildings in that campus are automatically assigned to the same virtual domain.
- When a building is assigned to a virtual domain, it automatically includes all of the floors associated with that building.
- When a floor is assigned, it automatically includes all of the access points associated with that floor.

Note If only floors are assigned to a virtual domain, you lose some ability to choose map-based features. For example, some reports and searches require you to drill down from campus to building to floor. Because campuses and buildings are not in the virtual domain, you are not able to generate these types of reports or searches.

Note Coverage areas shown in the NCS are only applied to campuses and buildings. In a floor-only virtual domain, the NCS does not display coverage areas.

Note If a floor is directly assigned to a virtual domain, it cannot be deleted from the virtual domain which has the building to which the floor belongs.

Note Search results do not display floor areas when the campus is not assigned to the virtual domain.

Access Points

When a controller or map is assigned to a virtual domain, the access points associated with the controller or map are automatically assigned as well. Access points can also be assigned manually (separate from the controller or map) to a virtual domain.

Note If the controller is removed from the virtual domain, all of its associated access points are also removed. If an access point is manually assigned, it remains assigned even if its associated controller is removed from the current virtual domain.

Note If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports.

Note If a manually added access point is removed from a virtual domain but is still associated with a controller or map that is assigned to the same virtual domain, the access point remains visible in the virtual domain. Any alarms associated with this access point are not deleted with the deletion of the access point.

Note When maps are removed from a virtual domain, the access points on the maps can be removed from the virtual domain.

Note If you later move an access point to another partition, some events (such as generated alarms) might reside in the original partition location.

Note Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, the NCS uses the detecting controller.
If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

Controllers

Because network elements are managed hierarchically, controllers might be affected by partitioning. If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports.

If you create a partition with only a few controllers, choose Configure > Access Points, and click an individual link in the AP Name column, the complete list of NCS-assigned controllers is displayed for primary, secondary, and tertiary controllers rather than the limited number specified in the partition.

Note If a controller configuration is modified by multiple virtual domains, complications might arise. To avoid this, manage each controller from only one virtual domain at a time.

Email Notification

E-mail notification can be configured per virtual domain. An e-mail is sent only when alarms occur in that virtual domain.

Creating a New Virtual Domain

Note See the "Managing a Virtual Domain" section on page 15-47 for more information.

To create a new virtual domain, follow these steps:

Step 1 Choose **Administration > Virtual Domains**.

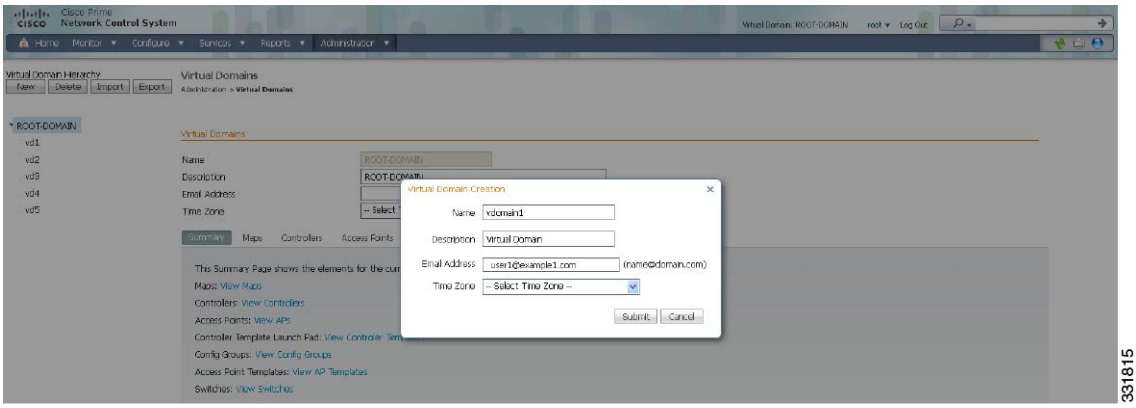
Step 2 From the Virtual Domain Hierarchy left sidebar menu, select the virtual domain to which you want to add a sub (child) virtual domain.

Note The selected virtual domain becomes the parent virtual domain of the newly created subvirtual domain.

Step 3 Click **New** (see Figure 15-4).

The Virtual Domain Creation pop-up dialog box appears.

Figure 15-4 Virtual Domains



Step 4 Enter the virtual domain name in the text box.

Step 5 Click **Submit** to create the virtual domain or **Cancel** to close the pop-up dialog box with no changes.

Note Each virtual domain might contain a subset of the elements included with its parent virtual domain. When a user is assigned a virtual domain, that user might view the same maps, controllers, and access points that are assigned to its parent virtual domain.

Note To modify or update a current virtual domain name or description, choose **Administration > Virtual Domains**. From the Virtual Domain Hierarchy left sidebar menu, choose the virtual domain you want to edit.

Managing a Virtual Domain

Choose a virtual domain from the Virtual Domain Hierarchy on the left sidebar menu to view or edit its assigned maps, controllers, access points, and switches. The Summary page appears. This page includes tabs for viewing the currently logged-in virtual domain-available maps, controllers, access points, and switches.

Note Because all maps, controllers, and access points are included in the partition tree, this page takes several seconds to load.

The Maps, Controllers, Access Points, and Switches tabs are used to add or remove components assigned to this virtual domain.

To assign a map, controller, or access point to this domain, follow these steps:

Step 1 Choose **Administration > Virtual Domains**.

Step 2 Choose a virtual domain hierarchy from the Virtual Domain Hierarchy left sidebar menu.

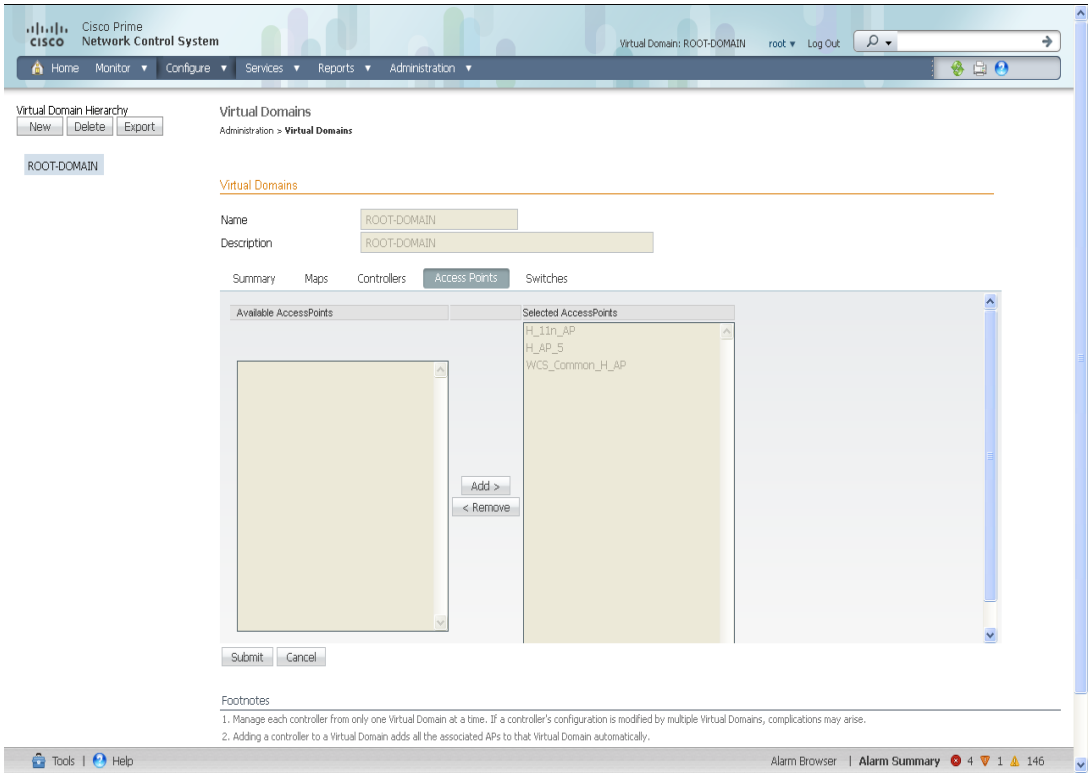
Note Because all maps, controllers, and access points are included in the partition tree, it takes several minutes to load. This time increases if you have a system with a significant number of controllers and access points.

Step 3 Click the applicable **Maps**, **Controller**, or **Access Points** tab.

Step 4 In the Available (Maps, Controllers, or Access Points) column, click to highlight the new component(s) you want to assign to the virtual domain.

Step 5 Click **Add** to move the component(s) to the Selected (Maps, Controllers, or Access Points) column (see Figure 15-5).

Figure 15-5 Virtual Domains Access Points Tab



Note To remove a component from the virtual domain, click to highlight the component in the Selected (Maps, Controllers, or Access Points) column, and click **Remove**. The component returns to the Available column.

Note If you delete a switch, a controller, or an autonomous AP from the ROOT-DOMAIN, the device is removed from the NCS. If the device is explicitly associated with the ROOT-DOMAIN and if you delete the device from a virtual domain, the device is removed from this virtual domain but it is not removed from the NCS.

Step 6 Click **Submit** to confirm the changes.

Note After assigning elements to a virtual domain and submitting the changes, the NCS might take some time to process these changes depending on how many elements are added.

Virtual Domain RADIUS and TACACS+ Attributes

The Virtual Domain Custom Attributes page allows you to indicate the appropriate protocol-specific data for each virtual domain. The Export button on the Virtual Domain Hierarchy left sidebar menu preformats the virtual domain RADIUS and TACACS+ attributes. You can copy and paste these attributes into the ACS server. This allows you to copy only the applicable virtual domains into the ACS server page and ensures that the users only have access to these virtual domains.

To apply the preformatted RADIUS and TACACS+ attributes to the ACS server, follow these steps:

Step 1 Choose **Administration > Virtual Domains**.

Step 2 From the Virtual Domain Hierarchy left sidebar menu, choose the virtual domain for which you want to apply the RADIUS and TACACS+ attributes.

Step 3 Click **Export**.

Step 4 Highlight the text in the RADIUS or TACACS+ Custom Attributes list (depending on which one you are currently configuring), go to menu of the browser, and choose **Edit > Copy**.

Step 5 Log in to ACS.

Step 6 Go to User or Group Setup.

Note If you want to specify virtual domains on a per-user basis, then you need to make sure you add all of the custom attributes (for example, tasks, roles, virtual domains) information to the User custom attribute page.

Step 7 For the applicable user or group, click **Edit Settings**.

Step 8 Use your browser Edit > Paste feature to place the RADIUS or TACACS+ custom attributes into the applicable field.

Step 9 Select the check boxes to enable these attributes.

Step 10 Click **Submit + Restart**.

Note For more information on adding RADIUS and TACACS+ attributes to the ACS server, see the "Adding NCS User Groups into ACS for TACACS+" section on page 15-105 or the "Adding NCS User Groups into ACS for RADIUS" section on page 15-109.

Understanding Virtual Domains as a User

When you log in, you can access any of the virtual domains that the administrator assigned to you.

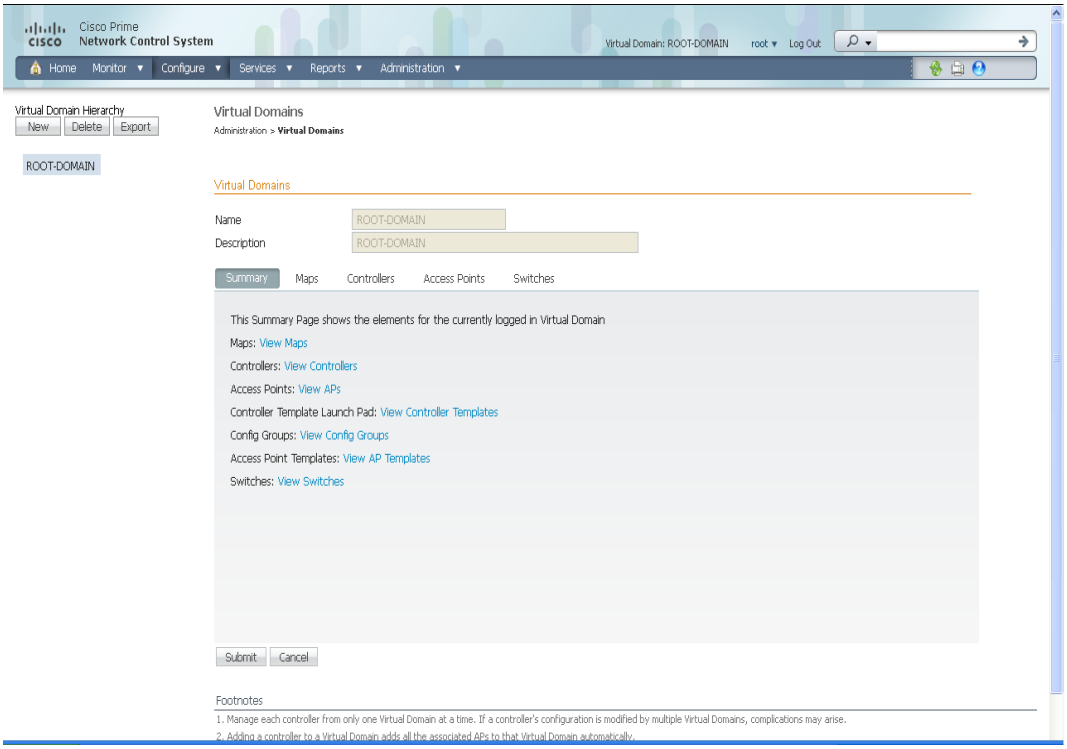
Only one virtual domain can be active at login. You can change the current virtual domain by using the Virtual Domain drop-down list at the top of the page. Only virtual domains that have been assigned to you are available in the drop-down list.

When you select a different virtual domain from the drop-down list, all reports, alarms, and other functionality are filtered by the conditions of the new virtual domain.

Viewing Assigned Virtual Domain Components

To view all components (including maps, controllers, access points, and switches) assigned to the current virtual domain, choose **Administration > Virtual Domains** (see Figure 15-6). Click a link on the Summary tab to view the assigned components for your virtual domain.

Figure 15-6 Virtual Domains Summary Tab



Limited Menu Access

Non-ROOT-DOMAIN virtual domain users do not have access to the following NCS menus:

- Monitor > RRM
- Configure > Auto Provisioning
- Configure > ACS View Servers
- Mobility > Mobility Services
- Mobility > Synchronize Servers
- Administration > Background Tasks

- Administration > Settings
- Administration > User Preferences
- Tools > Voice Audit
- Tools > Config Audit

Configuring Administrative Settings

Settings contain options for managing the NCS data retention functions. This section describes the sets of options that are available and contains the following topics:

Configuring Alarms

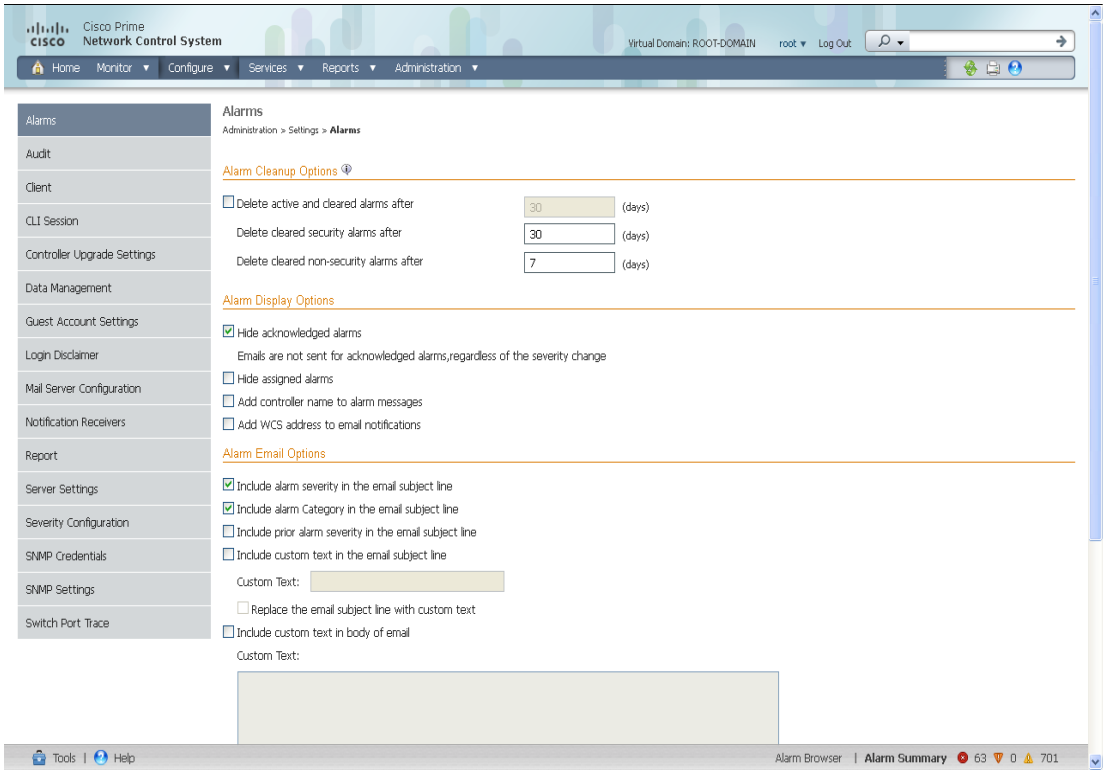
This Alarms page enables you to handle old alarms and display assigned and acknowledged alarms in the Alarm Summary page.

To open this page, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Alarms**. The Administration > Settings > Alarms page appears (see Figure 15-7).

Figure 15-7 Settings > Alarms Page



Step 3 Add or modify the following Alarms parameters:

- Alarm Cleanup Options
  - Delete active and cleared alarms after—Enter the number of days after which active and cleared alarms are deleted. This option can be disabled by unselecting the check box.
  - Delete cleared security alarms after—Enter the number of days after which Security, Rogue AP, and Adhoc Rogue alarms are deleted.
  - Delete cleared non-security alarms after—Enter the number of days after which non-security alarms are deleted. Non-security alarms include all alarms that do not fall under the Security, Rogue AP, or Adhoc Rogue categories.

Note Data cleanup tasks run nightly to delete old alarms. In addition to the data cleanup task, the NCS has an hourly task to check alarm table size. When the alarm table size exceeds 300 K, the task deletes the oldest cleared alarms until the alarm table size is within 300 K.

Note If you want to keep the cleared alarms for more than 7 days, then you can specify a value more than 7 days in the Delete cleared non-security alarms after text box until the alarm table size reaches 300 K.

- Alarm Display Options

Note These preferences only apply to the Alarm Summary page. Quick searches or alarms for any entity display all alarms regardless of the acknowledged or assigned state.

  - Hide acknowledged alarms—When the check box is selected, Acknowledged alarms do not appear on the Alarm Summary page. This option is enabled by default.

    Note E-mails are not generated for acknowledged alarms regardless of severity change.

  - Hide assigned alarms—When the check box is selected, assigned alarms do not appear in the Alarm Summary page.
  - Add controller name to alarm messages—Select the check box to add the name of the controller to alarm messages.
  - Add NCS address to e-mail notifications—Select the check box to add the NCS address to e-mail notifications.

- Alarm E-mail Options
  - Include alarm severity in the e-mail subject line—Select the check box to include alarm severity in the e-mail subject line.
  - Include alarm Category in the e-mail subject line—Select the check box to include alarm category in the e-mail subject line.
  - Include prior alarm severity in the e-mail subject line—Select the check box to include prior alarm severity in the e-mail subject line.
  - Include custom text in the e-mail subject line—Select the check box to add custom text in the e-mail subject line. You can also replace the e-mail subject line with custom text by selecting the Replace the e-mail subject line with custom text check box.
  - Include custom text in body of e-mail—Select the check box to add custom text in the body of e-mail.
  - Include alarm condition in body of e-mail—Select the check box to include alarm condition in the body of e-mail.
  - Add link to Alarm detail page in body of e-mail—Select the check box to add a link to the Alarm detail page in the body of e-mail.
  - Enable Secure Message Mode—Select the check box to enable a secure message mode. If you select the Mask IP Address and Mask Controller Name check boxes, the alarm e-mails are sent in secure mode where all the IP addresses and controller names are masked.

Step 4 Click **Save**.

Configuring an Audit

The Settings > Audit page allows you to determine the type of audit and on which parameters the audit is performed.

- Audit Mode—Choose between basic auditing and template based auditing.
- Audit On—Choose to audit on all parameters or on selected parameters for a global audit.

Audit Mode

The audit mode group box allows you to choose between basic auditing and template based auditing. Basic audit is selected by default.

- Basic Audit—Audits the configuration objects in the NCS database against current WLC device values. Prior to the 5.1.0.0 version of the NCS, this was the only audit mode available.

Note Configuration objects refer to the device configuration stored in the NCS database.

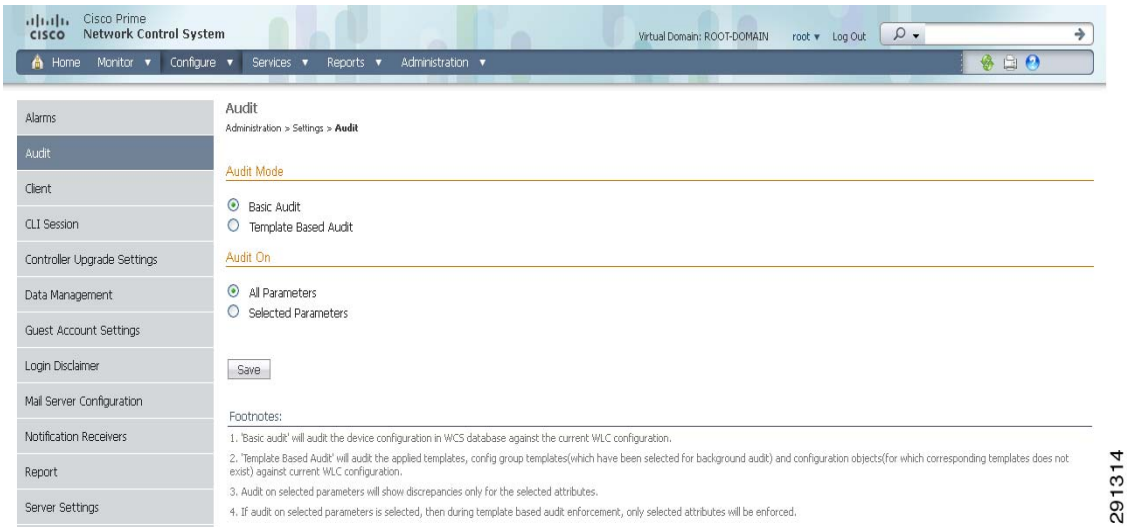
- Template-based Audit—Audits on the applied templates, config group templates (which have been selected for the background audit), and configuration audits (for which corresponding templates do not exist) against current Controller device values.

To indicate the type of audit you want to perform, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Audit**. The Audit Setting page appears (see Figure 15-8).

Figure 15-8 Audit Settings Page



Step 3 Select the **Basic Audit** or **Template Based Audit**. A basic audit audits the device configuration in the NCS database against the current Controller configuration. A template-based audit audits the applied templates, config group templates, and configuration objects (for which corresponding templates do not exist) against current Controller configuration.

Step 4 Choose if you want the audit to run on all parameters or only on selected parameters. If you select the Selected Parameters radio button, you can access the Configure Audit Parameters configuration page. (See the "Configuring Audit Parameters" section on page 15-55). The Select audit parameters URL appears.

The selected audit parameters are used during network and controller audits.

Step 5 Click **Save**.

Note These settings are in effect when the controller audit or network audit is performed.

Audit On

The Audit On group box allows you to audit on all parameters or to select specific parameters for an audit. When the Selected Parameters radio button is selected, you can access the Select Audit Parameters configuration page.

The selected audit parameters are used during network and controller audits.

Configuring Audit Parameters

To configure the audit parameters for a global audit, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Audit**.

Step 3 Select the **Selected Parameters** radio button to display the Select Audit Parameters link.

Step 4 Click **Save**.

Step 5 Click **Select Audit Parameters** to choose the required parameters for the audit in the Audit Configuration > Parameter Selection page.

Step 6 Select the parameters that you want audited from each of the tabs. The tabs include System, WLAN, Security, Wireless, and Selected Attributes.

Step 7 When all desired audit parameters are selected, click **Submit** to confirm the parameters or click **Cancel** to close the page without saving any audit parameters.

Once you click **Submit**, the selected audit parameters display on the Selected Attributes tab.

A current Controller Audit Report can be accessed from the Configure > Controllers page by selecting an object from the Audit Status column.

Note You can audit a controller by choosing **Audit Now** from the Select a command drop-down list in the Configure > Controllers page, or by clicking **Audit Now** directly from the Controller Audit report. See the "Viewing Audit Status (for Access Points)" section on page 8-196.

Configuring Clients

You can configure the following client processes to improve NCS performance and scalability. This section contains the following topics:

- Client Traps and Syslogs, page 15-58
- Autonomous Client Traps, page 15-58

To confirm changes to these client configurations, click **Save** at the bottom of the page.

Note See the "Client Troubleshooting Dashlet" section on page 9-4 for further information on client troubleshooting.

Processing Diagnostic Trap

The Settings > Client page allows you to enable automatic client troubleshooting on a diagnostic channel.

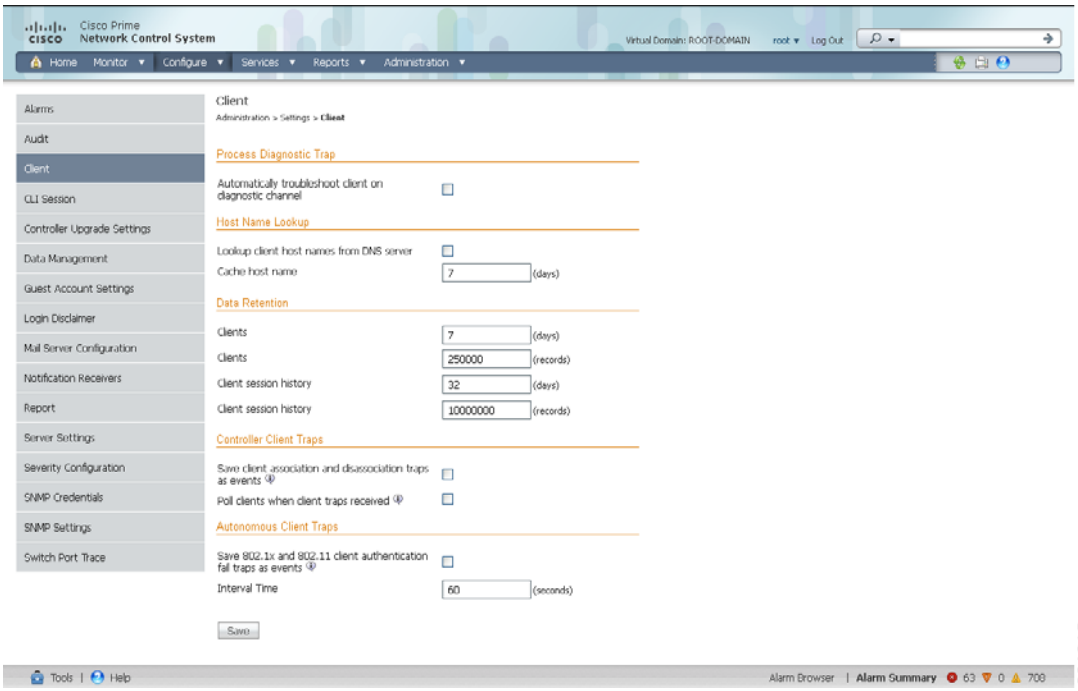
Note Automatic client troubleshooting is only available for CCXV5 or CCXv6 clients.

To enable this automatic client troubleshooting, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Client**. The Client page appears (see Figure 15-9).

Figure 15-9 Administration > Settings > Client Page



Step 3 Select the **Automatically troubleshoot client on diagnostic channel** check box.

Note If the check box is selected, the NCS processes the diagnostic association trap. If it is not selected, the NCS raises the trap, but automated troubleshooting is not initiated.

Note While processing the diagnostic association trap, the NCS invokes a series of tests on the client. The client is updated on all completed tasks. The automated troubleshooting report is placed in dist/acs/win/webnms/logs. When the test is complete, the location of the log is updated in client details pages:V5 tab:Automated Troubleshooting Report group box. An export button allows you to export the logs.

Step 4 Click **Save**.

Host Name Lookup

DNS lookup can take a considerable amount of time. Because of this, you can enable or disable the DNS lookup for client host name. It is set to Disable by default.

To enable host name lookup, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Client**.

Step 3 Select the **Lookup client host names from DNS server** check box.

Step 4 Enter the number of days that you want the host name to remain in the cache.

Step 5 Click **Save**.

Data Retention

Client association history can take a lot of database and disk space. This can be an issue for database backup and restore functions. The retaining duration of a client association history can be configured to help manage this potential issue.

To configure data retention parameters, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Client**.

Step 3 Enter or edit the following data retention parameters:

- Dissociated Clients (days)—Enter the number of days that you want NCS to retain the data. The default is 7 days. The valid range is 1 to 30 days.
- Client session history (days)—Enter the number of days that you want NCS to retain the data. The default is 32 days. The valid range is 7 to 365 days.

Step 4 Click **Save**.

Client Discovery

If you select the **Poll clients when client traps/syslogs received** check box, the NCS polls clients to quickly identify client sessions. In a busy network, you might want to disable polling while the client traps are received. This option is disabled by default.

Client Traps and Syslogs

In some deployments, the NCS might receive large amounts of client association and disassociation traps. Saving these traps as events might cause a slight performance issue. In such cases, other events that might be useful might be aged out sooner than expected.

To ensure that the NCS does not save client association and disassociation traps as events, unselect the **Save client association and disassociation traps as events** check box. Click **Save** to confirm this configuration change. This option is disabled by default.

For more information on traps and syslogs, see the "Enabling Traps and Syslogs on Switches for Wired Client Discovery" section on page 8-208.

Autonomous Client Traps

Select the **Save 802.1x and 802.11 client authentication fail traps as events** check box if you want to save the Save 802.1x and 802.11 client authentication failed traps as events.

Interval Time—Enter the time interval in seconds to poll for the failed traps.

Configuring Protocols for CLI Sessions

Many NCS features such as autonomous access point and controller command-line interface templates, along with migration templates require executing command-line interface commands on the autonomous access point or controller. These command-line interface commands can be executed by establishing Telnet or SSH sessions. The CLI session page allows you to select the session protocol. SSH is the default.

Note In command-line interface templates, you are not required to answer the question responses (such as *Yes* or *No* answer to a command, *Press enter to continue*, and so on.). This is automatically performed by the NCS.

To configure the protocols for CLI sessions, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **CLI Session**.

Step 3 The default controller session protocol SSH is selected. To choose Telnet, select that radio button.

Step 4 The default autonomous access point session protocol SSH is selected. To choose Telnet, select the radio button.

Step 5 The **Run Autonomous AP Migration Analysis on discovery** radio button is set to **No** by default. Choose **Yes** if you want to discover the autonomous APs as well as perform migration analysis.

Step 6 Click **Save**.

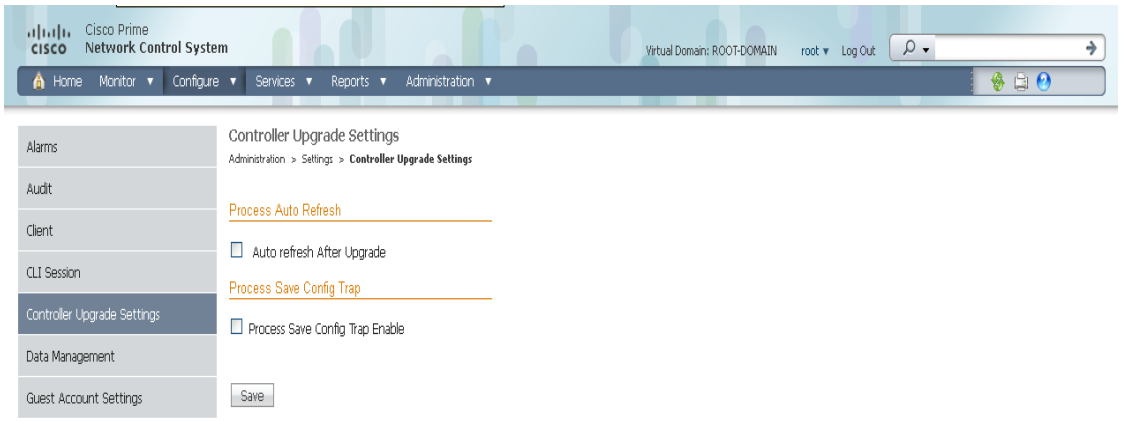
Configuring Controller Upgrade

The Controller Upgrade Settings page allows you to auto-refresh after a controller upgrade. To perform an auto-refresh, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Controller Upgrade Settings** (see Figure 15-10).

Figure 15-10 Controller Upgrade Settings



Step 3 Select the **Auto refresh After Upgrade** check box to automatically restore the configuration whenever there is a change in the controller image.

Step 4 Determine the action the NCS takes when a save config trap is received. When this check box is enabled, you can choose to retain or delete the extra configurations present on the device but not on the NCS. The setting is applied to all controllers managed by the NCS.

Note If you select the Auto Refresh on Save Config Trap check box in the Configure > Controllers > Properties > Settings page, it overrides this global setting.

Note It might take up to three minutes for the automatic refresh to occur.

Step 5 Click **Save**.

Whenever a save config trap is received by the NCS this check box is selected. When this check box is enabled, it determines the action taken by the NCS.

When this check box is enabled, the user can choose to retain or delete the extra configurations present on device and not on the NCS.

This setting is applied to all of the controllers managed by the NCS. The setting in the controller > properties page for processing the save config trap overrides this global setting.

When there is a change in the controller image, the configuration from the controller is automatically restored.

Configuring Data Management

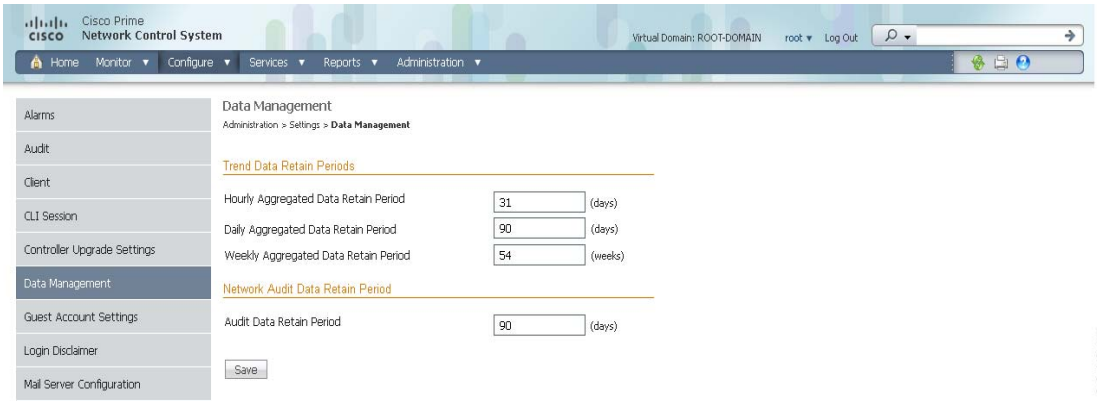
You can configure retention periods on an hourly, daily, and weekly basis.

To set retention periods for aggregated data used in timed calculations and network audit calculations, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Data Management**. The Data Management page appears (see Figure 15-11).

Figure 15-11 Data Management Page



Step 3 Specify the number of days to keep the hourly data. The valid range is 1 to 31. The default is 31 days.

Step 4 Specify the number of days to keep the daily data. The valid range is 7 to 365. The default is 90 days.

Step 5 Specify the number of weeks to keep the weekly data. The valid range is 2 to 108. The default is 54 weeks.

Step 6 Specify the number of days to retain the audit data collected by the Network Audit background task before purging. The limit is 365 days, and the minimum cleanup interval is 7 days. The default is 90 days.

Note For the best interactive graph data views, change the default settings to the maximum possible: 90 days for daily aggregated data and 54 weeks for weekly aggregated data. You must also make the appropriate measures to increase RAM and CPU capacity to compensate for these adjustments.

Step 7 Click **Save**.

NCS Historical Data

There are two types of historical data in the NCS, including the following:

- Aggregated historical data—Numeric data that can be gathered as a whole and aggregated to minimum, maximum, or average. Client count is one example of aggregated historical data.

  Use the Administration > Settings > Data Management page to define the aggregated data retention period. Aggregation types include hourly, daily, and weekly.

  The retention period for these aggregation types are defined as Default, Minimum, and Maximum (see Table 15-3).

Table 15-3 Aggregated Data Retention Periods

Aggregated Data	Default	Minimum	Maximum
Hourly	31 days	1 day	31 days
Daily	90 days	7 days	365 days
Weekly	54 weeks	2 weeks	108 weeks

- Non-aggregated historical data—Numeric data that cannot be gathered as a whole (or aggregated). Client association history is one example of non-aggregated historical data.

  You can define a non-aggregated retention period in each data collection task and other settings.

  For example, you define the retention period for client association history in Administration > Settings > Client. By default, the retention period is 31 days or 1 million records. This retention period can be increased to 365 days.

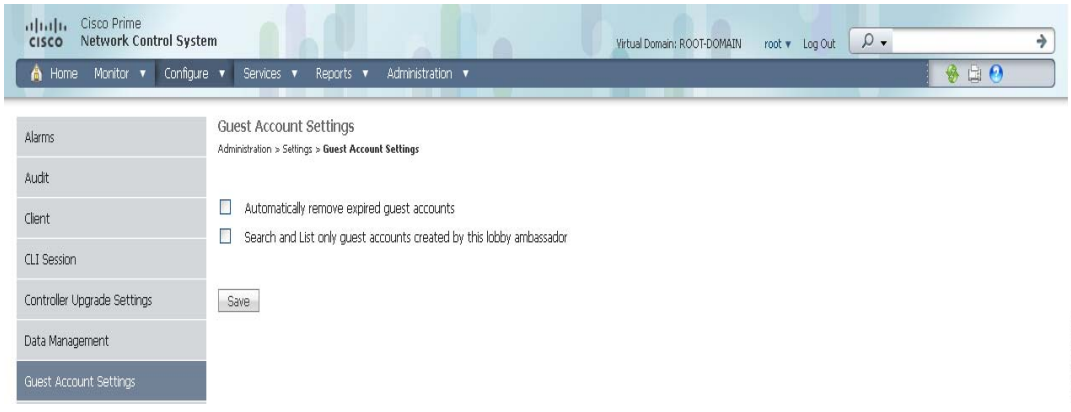
Configuring Guest Account Settings

The Guest Account Settings page allows you to globally remove all expired templates. To configure guest account settings, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Guest Account Settings** (see Figure 15-12).

Figure 15-12 Guest Account Settings Page



Step 3 When the **Automatically remove expired guest accounts** check box is selected, the guest accounts whose lifetime has ended are not retained, and they are moved to the Expired state. Those accounts in the expired state are deleted from the NCS.

Step 4 By default, the NCS Lobby Ambassador can access all guest accounts irrespective of who created them. If you select the **Search and List only guest accounts created by this lobby ambassador** check box, the Lobby Ambassadors can access only the guest accounts that have been created by them.

Step 5 Click **Save**.

Configuring Login Disclaimer

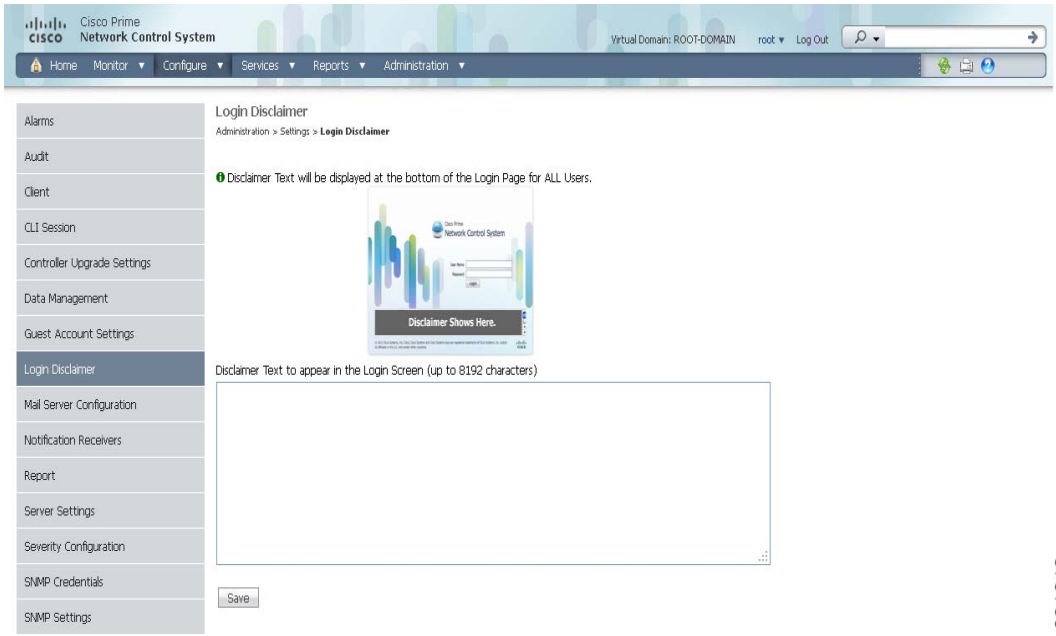
The Login Disclaimer page allows you to enter disclaimer text at the top of the Login page for all users.

To enter Login Disclaimer text, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Login Disclaimer**. The Login Disclaimer page appears (see Figure 15-13).

Figure 15-13 Login Disclaimer Page



Step 3 Enter your Login Disclaimer text in the available text box.

Step 4 Click **Save**.

Configuring the Mail Server

You can configure global e-mail parameters for sending e-mails from NCS reports, alarm notifications, and so on. This mail server page enables you to configure e-mail parameters in one place. The Mail Server page enables you to set the primary and secondary SMTP server host and port, the e-mail address of the sender, and the e-mail addresses of the recipient.

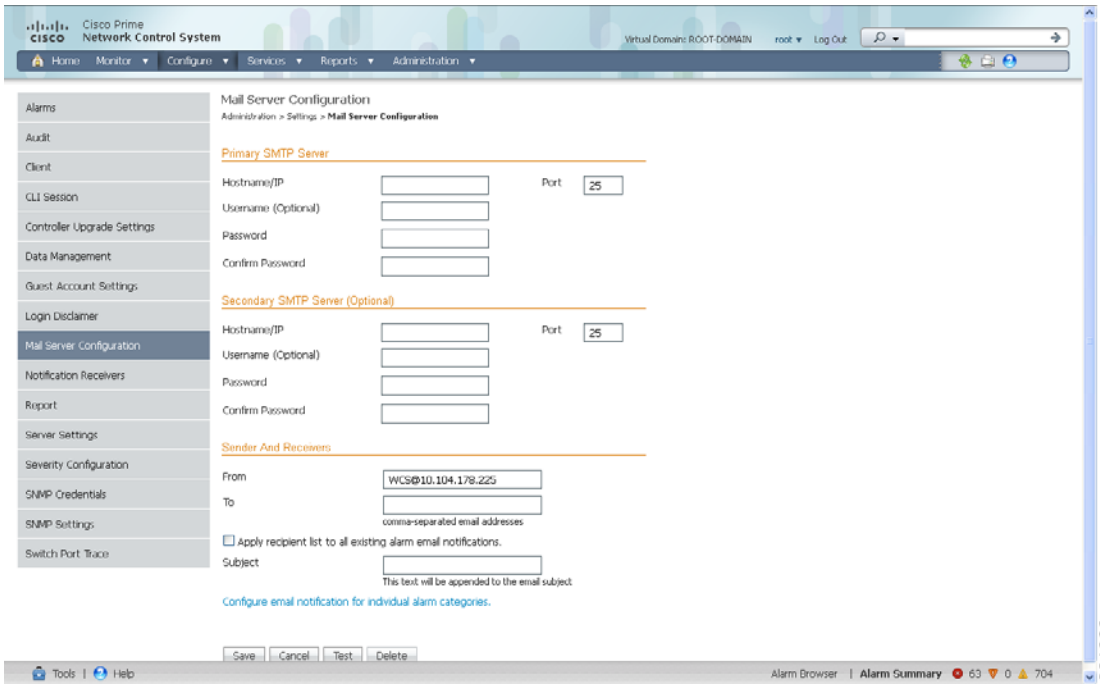
To configure global e-mail parameters, follow these steps:

Note You must configure the global SMTP server before setting global e-mail parameters.

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Mail Server Configuration**. The page in Figure 15-14 appears.

Figure 15-14 Mail Server Configuration Page



Step 3 Enter the hostname of the primary SMTP server.

Step 4 Enter the username of the SMTP server.

Step 5 Provide a password for logging on to the SMTP server and confirm it.

Note Both Username and Password are optional.

Step 6 Provide the same information for the secondary SMTP server (only if a secondary mail server is available).

Step 7 The From text box in the Sender and Receivers portion of the page is populated with *NCS@<NCS server IP address>*. You can change it to a different sender.

Step 8 Enter the e-mail addresses of the recipient in the To text box. The e-mail address you provide serves as the default value for other functional areas, such as alarms or reports. Multiple e-mail addresses can be added and should be separated by commas.

Note Global changes you make to the recipient e-mail addresses in Step 7 are disregarded if e-mail notifications were set.

You must indicate the primary SMTP mail server and fill the From address text boxes.

If you want all alarm categories applied to the provided recipient list, select the **Apply recipient list to all alarm categories** check box.

Step 9 Enter the text that you want to append to the e-mail subject.

Step 10 If you click the Configure e-mail notification for individual alarm categories link, you can specify the alarm categories and severity levels you want to enable. E-mail notifications are sent when an alarm occurs that matches categories and the severity levels you select.

Note You can set each alarm severity by clicking the alarm category, choosing Critical, Major, Minor, or Warning, and providing an e-mail address.

Step 11 Click the **Test** button to send a test e-mail using the parameters you configured. The results of the test operation appear on the same page. The test feature checks the connectivity to both primary and secondary mail servers by sending an e-mail with a "NCS test e-mail" subject line.

If the test results were satisfactory, click **Save**.

Configuring the Notification Receiver

The Notification Receiver page displays current notification receivers that support guest access. Alerts and events are sent as SNMPv2 notifications to configured notification receivers.

In this page, you can view current or add additional notification receivers.

This section contains the following topics:

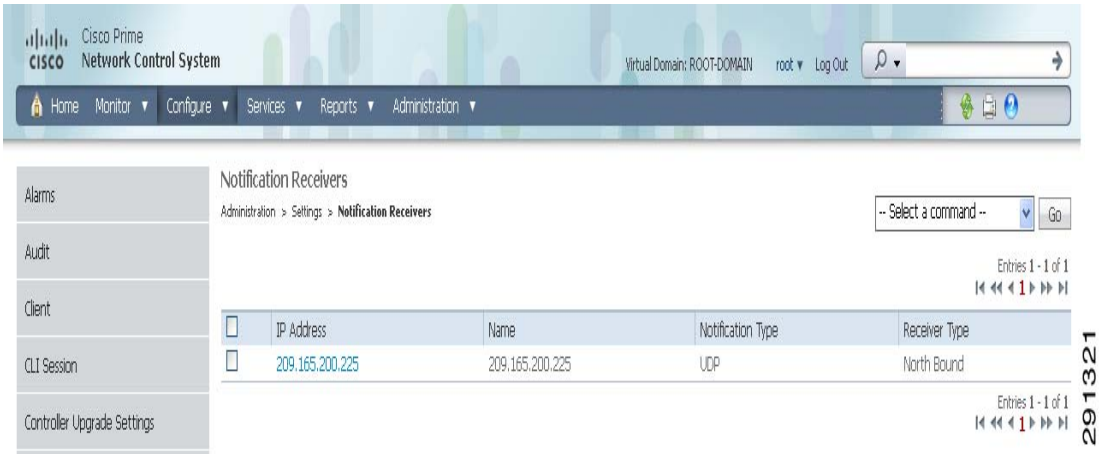
- Adding a Notification Receiver to the NCS, page 15-65
- Removing a Notification Receiver, page 15-66

To access the Notification Receiver page, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Notification Receivers**. All currently configured servers appear in this page. If you want to add one, choose **Add Notification Receiver** from the Select a command drop-down list, and click **Go** (see Figure 15-15).

Figure 15-15 Notification Receiver Page



Adding a Notification Receiver to the NCS

To view current or add additional notification receivers, follow these steps:

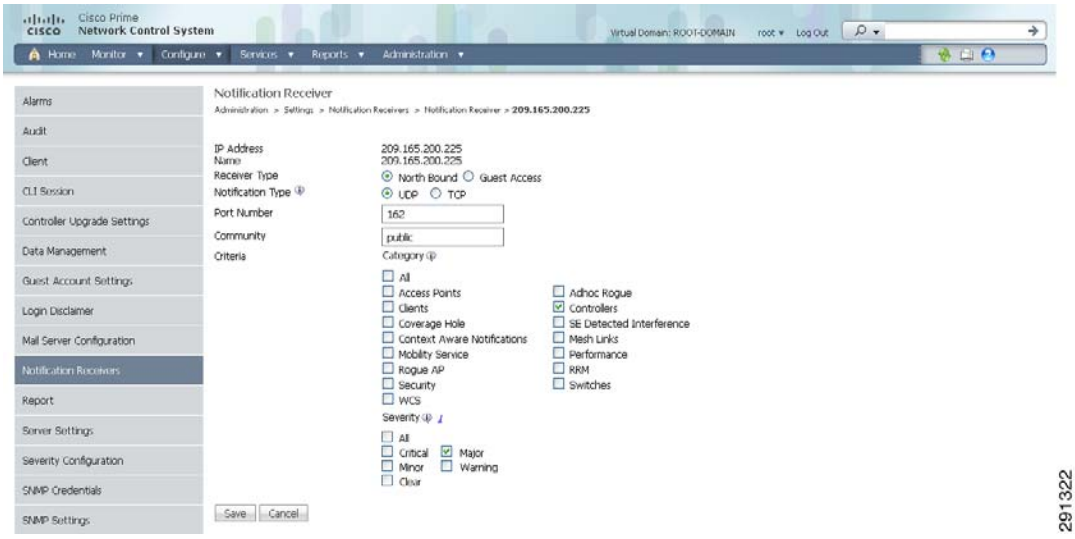
Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Notification Receivers**. All currently configured servers appear on this page.

Step 3 From the Select a command drop-down list, choose **Add Notification Receiver**.

Step 4 Click **Go** (see Figure 15-15).

Figure 15-16 Notification Receiver Page



Step 5 Enter the server IP address and name.

Step 6 Select either the **North Bound** or **Guest Access** radio button.

The Notification Type automatically defaults to UDP.

Step 7 Enter the UDP parameters including Port Number and Community.

Note The receiver that you configure should be listening to UDP on the same port that is configured.

Step 8 If you selected North Bound as the receiver type, specify the criteria and severity.

Note Alarms for only the selected category are processed.

Note Alarms with only the selected severity matching the selected categories are processed.

Step 9 Click **Save** to confirm the Notification Receiver information.

Note
- By default, only INFO level events are processed for the selected Category.
- Only SNMPV2 traps are considered for North Bound notification.

Removing a Notification Receiver

To delete a notification receiver, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Notification Receivers**. All currently configured servers appear on this page.

Step 3 Select the check box(es) of the notification receiver(s) that you want to delete.

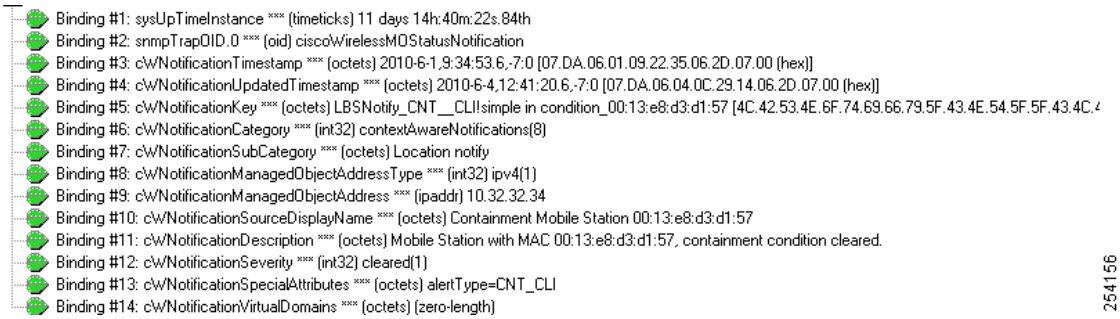
Step 4 From the Select a command drop-down list, click **Remove Notification Receiver**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion.

The sample display from a North Bound SNMP receiver that has received event traps from the NCS follows:

Figure 15-17 Sample Display from a North Bound SNMP Receiver



The following sample output shows the log file generated by the NCS. This log file is located in the log file directory on the NCS server (/opt/NCS 1.x/webnms/logs). The log output helps you troubleshoot when alarms are not being received by the North Bound SNMP receiver.

```
06/04/10 08:30:58.559 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]Adding into queue
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrTotalNotifications2
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrHandledInNotification2
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrNonCongestedIn2
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService][addNBAlert]Added into queue
06/04/10 08:30:58.561 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][getNbAlarm]incrHandledOutNotification2
06/04/10 08:30:58.561 INFO[com.cisco.ncslogger.services] :
[NBNotificationService][startNotifier]Processing the
alertNoiseProfile_LradIf!00:17:df:a9:c8:30!0
06/04/10 08:30:58.561 INFO[com.cisco.ncslogger.notification] :
[NbAlertToNmsAlertCorrelator][formVarBindList]Generating the varbind list for NB
06/04/10 08:30:58.562 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.2.1.1.3.0 variable value: 10 days, 20:22:17.26
06/04/10 08:30:58.562 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.6.3.1.1.4.1.0 variable value:
1.3.6.1.4.1.9.9.199991.0.1
06/04/10 08:30:58.562 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.2 variable value:
07:da:05:18:0c:30:0d:09:2d:07:00
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.3 variable value:
07:da:06:04:08:1e:3a:04:2d:07:00
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.4 variable value:
NoiseProfile_LradIf!00:17:df:a9:c8:30!0
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.5 variable value: 2
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.6 variable value: Radio
load threshold violation
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.7 variable value: 1
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.8 variable value:
172.19.29.112
```

```
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.9 variable value: AP
1250-LWAP-ANGN-170-CMR, Interface 802.11b/g/n
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.10 variable value:
Noise changed to acceptable level on '802.11b/g/n' interface of AP
'1250-LWAP-ANGN-170-CMR', connected to Controller '172.19.29.112'.
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.11 variable value: 1
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.12 variable value:
06/04/10 08:30:58.565 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.14 variable value:
06/04/10 08:30:58.573 INFO[com.cisco.ncslogger.notification] : [NBUtil][sendTrap]OSS list
size with reachability status as up1
06/04/10 08:30:58.573 INFO[com.cisco.ncslogger.notification] : [NBUtil][sendTrap]Sending
UDP Notification for receiver:172.19.27.85 on port:162
```

MIB to NCS Alert/Event Mapping

Table 15-4 summarizes the Cisco-NCS-Notification-MIB to NCS alert/event mapping.

Table 15-4 Cisco-NCS-Notification-MIB to NCS Alert/Event Mapping

Field Name and Object ID	Data Type	NCS Event/Alert field	Description
cWNotificationTimestamp	DateAndTime	createTime - NmsAlert eventTime - NmsEvent	Creation time for alarm/event.
cWNotificationUpdatedTimestamp	DateAndTime	modTime - NmsAlert	Modification time for Alarm. Events do not have modification time.
cWNotificationKey	SnmpAdminString	objectId - NmsEvent entityString- NmsAlert	Unique alarm/event ID in string form.
cWNotificationSubCategory	OCTET STRING	Type field in alert and eventType in event.	This object represents the subcategory of the alert.
cWNotificationServerAddress	InetAddress	N/A	NCS IP address.

Table 15-4 Cisco-NCS-Notification-MIB to NCS Alert/Event Mapping (continued)

Field Name and Object ID	Data Type	NCS Event/Alert field	Description
cWNotificationManagedObject AddressType	InetAddressType	N/A	The type of Internet address by which the managed object is reachable. Possible values: 0 - unknown 1 - IPv4 2 - IPv6 3 - IPv4z 4 - IPv6z 16 - DNS Always set to "1" because NCS only supports ipv4 addresses.
cWNotificationManagedObject Address	InetAddress	getNode() value is used if present	getNode is populated for events and some alerts. If it is not null, then it is used for this field.
cWNotificationSourceDisplayName	OCTET STRING	sourceDisplayName field in alert/event.	This object represents the display name of the source of the notification.
cWNotificationDescription	OCTET STRING	Text - NmsEvent Message - NmsAlert	Alarm description string.
cWNotificationSeverity	INTEGER	severity - NmsEvent, NmsAlert	Severity of the alert/event critical(1), major(2), minor(3), warning(4), clear(5), info(6), unknown(7).

Table 15-4 Cisco-NCS-Notification-MIB to NCS Alert/Event Mapping (continued)

Field Name and Object ID	Data Type	NCS Event/Alert field	Description
cWNotificationSpecialAttributes	OCTET STRING	All the attributes in alerts/events apart from the base alert/event class.	This object represents the specialized attributes in alerts like APAssociated, APDisassociated, RogueAPAlert, CoverageHoleAlert, and so on. The string is formatted in 'property=value' pairs in CSV format.
cWNotificationVirtualDomains	OCTET STRING	N/A	Virtual Domain of the object that caused the alarm. This field is not populated for running release and this is populated with empty string.

Configuring Reports

To indicate where the scheduled reports reside and for how many days, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Report**. The Report page appears (see Figure 15-18).

Figure 15-18 Report Page

Step 3 Enter the path for saving report data files on a local PC. You can edit the existing default path.

Step 4 Specify the number of days to retain report data files.

Step 5 Click **Save**.

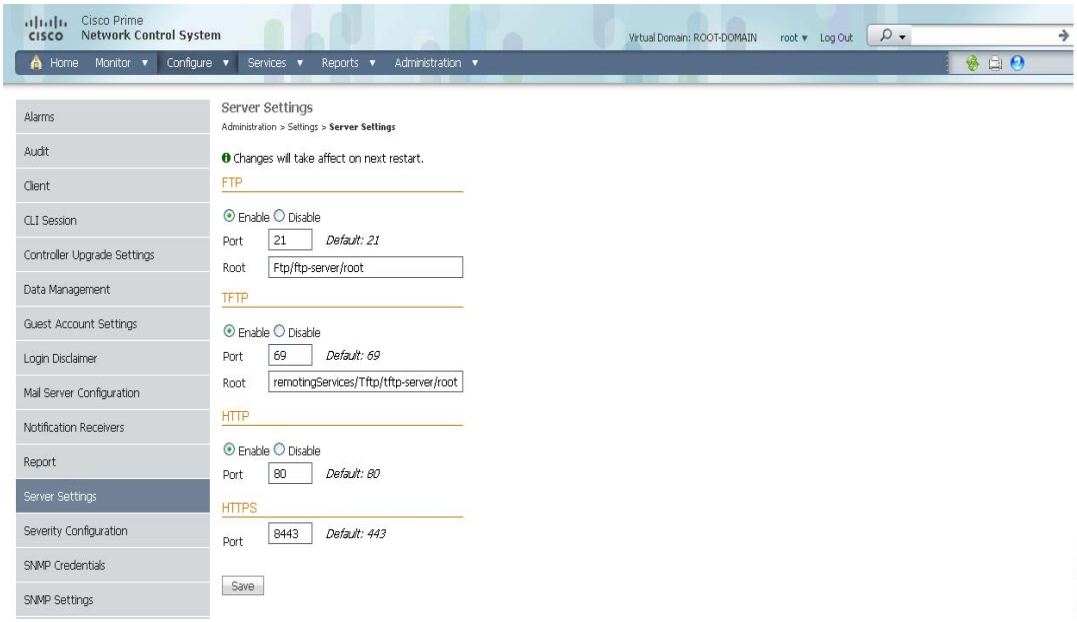
Configuring Server Settings

To turn TFTP, FTP, HTTP, or HTTPS on or off, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Server Setting**. The Server Settings page appears (see Figure 15-19).

Figure 15-19 Server Settings Page



Step 3 If you want to modify the FTP and TFTP directories or the HTTP and HTTPS ports that were established during installation, enter the port number (or port number and root where required) that you want to modify and click **Enable** or **Disable**.

The changes are reflected after a restart.

Configuring Alarm Severities

You can change the severity level for newly generated alarms.

Note Existing alarms remain unchanged.

To change the severity level of newly generated alarms, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 Choose **Severity Configuration** from the left sidebar menu. The Severity Configuration page appears (see Figure 15-20).

Figure 15-20 Severity Configuration Page

Step 3 Select the check box of the alarm condition whose severity level you want to change.

Step 4 From the Configure Severity Level drop-down list, choose the new severity level (Critical, Major, Minor, Warning, Informational, Reset to Default).

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the change.

Configuring SNMP Credentials

The SNMP Credentials page allows you to specify credentials to use for tracing the rogue access points. Use this option when you cannot find a specific entry using a number-based entry. When a switch credential is not added to the NCS, you can use SNMP credentials on this page to connect to the switch.

To configure SNMP credentials, follow these steps:

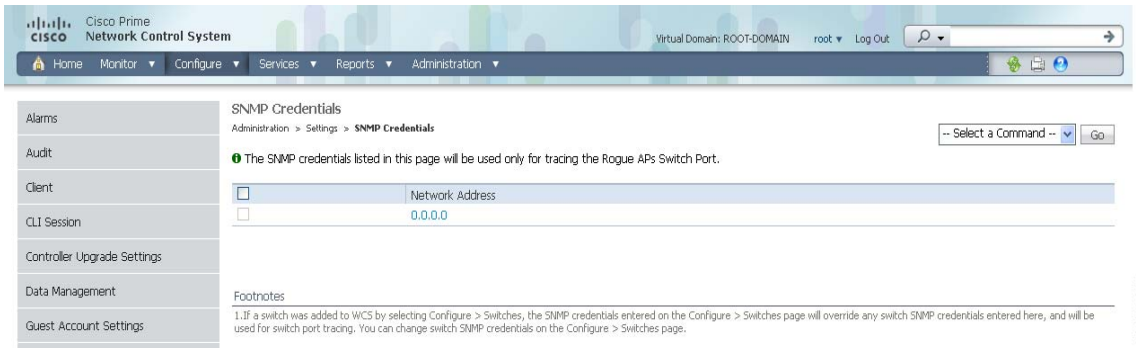
Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **SNMP Credentials**. The SNMP Credentials page appears (see Figure 15-21).

Step 3 To view or edit details about a current SNMP entry, click the **Network Address** link. See the "Viewing Current SNMP Credential Details" section on page 15-73 for more information.

Note The default network address is 0.0.0.0 which indicates the entire network. An SNMP credential is defined per network so only network addresses are allowed. 0.0.0.0 is the SNMP credential default and is used when no specific SNMP credential is defined. The default community string is *private* for both read and write. You should update the prepopulated SNMP credential with your own SNMP information.

Figure 15-21 SNMP Credentials Page



291327

Step 4 To add a new SNMP entry, choose **Add SNMP Entries** from the Select a command drop-down list, and click **Go**. See the "Adding a New SNMP Credential Entry" section on page 15-74 for more information.

Viewing Current SNMP Credential Details

To view or edit details for current SNMP credentials, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **SNMP Credentials**.

Step 3 Click the Network Address link to open the SNMP Credential Details page. The details page displays the following information:

General Parameters

- Add Format Type—Display only. See the "Adding a New SNMP Credential Entry" section on page 15-74 for more information regarding Add Format Type.
- Network Address
- Network Mask

SNMP Parameters—Select the applicable version(s) for SNMP parameters. The SNMP credentials are validated according to which SNMP version(s) are selected.

Note Enter SNMP parameters for write access, if available. With Display only access parameters, the switch is added but you cannot modify its configuration in the NCS. Device connectivity tests use the SNMP retries and timeout parameters configured in Administration > Settings > SNMP Settings.

- Retries—The number of times that attempts are made to discover the switch.
- Timeout—The session timeout value in seconds. This determines the maximum amount of time allowed for a client before it is forced to reauthenticate.
- SNMP v1 Parameters or v2 Parameters—If selected, enter the applicable community in the available text box.
- SNMP v3 Parameters—If selected, configure the following parameters:
  - Username
  - Auth. Type
  - Auth. Password
  - Privacy Type
  - Privacy Password

Note If SNMP v1 or v2 with default community is configured, the network is open to easy attacks because default communities are well known. SNMP v1 or v2 with a non-default community is more secure than a default community, but SNMP v3 with Auth and Privacy type and no default user is the most secure SNMP connection.

Step 4 Click **OK** to save changes or **Cancel** to return to the SNMP Credentials page without making any changes to the SNMP credential details.

Adding a New SNMP Credential Entry

To add a new SNMP credential entry, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **SNMP Credentials**.

Step 3 From the Select a command drop-down list, choose **Add SNMP Entries**.

Step 4 Click **Go**. The SNMP Credentials page opens (see Figure 15-21).

Step 5 Choose one of the following:

To manually enter SNMP credential information, leave the Add Format Type drop-down list at SNMP Credential Info. To add multiple network addresses, use a comma between each address. Go to Step 7.

If you want to add multiple switches by importing a CSV file, choose **File** from the Add Format Type drop-down list. The CSV file allows you to generate your own import file and add the devices you want. Go to Step 6.

Step 6 If you chose File, click **Browse** to find the location of the CSV file you want to import. Skip to Step 11.

The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory.

Sample File:

```
ip_address,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmpv3_auth_passw
ord,snmpv3_privacy_type,snmpv3_privacy_password,network_mask
1.1.1.0,v2,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.0
2.2.2.0,v2,private,user1,HMAC-MD5,password3,DES,password4,255.255.255.0
10.77.246.0,v2,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.0
```

The CSV file can contain the following fields:

- ip_address:IP address
- snmp_version:SNMP version
- network_mask:Network mask
- snmp_community:SNMP V1/V2 community
- snmpv3_user_name:SNMP V3 username
- snmpv3_auth_type:SNMP V3 authorization type. Can be None or HMAC-MD5 or HMAC-SHA
- snmpv3_auth_password:SNMP V3 authorization password
- snmpv3_privacy_type:SNMP V3 privacy type. Can be None or DES or CFB-AES-128
- snmpv3_privacy_password:SNMP V3 privacy password
- snmp_retries:SNMP retries
- snmp_timeout:SNMP timeout

Step 7 If you chose SNMP Credential Info, enter the IP address of the switch you want to add. If you want to add multiple switches, use a comma between the string of IP addresses.

Step 8 In the Retries field, enter the number of times that attempts are made to discover the switch.

Step 9 Provide the session timeout value in seconds. This determines the maximum amount of time allowed for a client before it is forced to reauthenticate.

Step 10 Select the applicable version(s) for SNMP parameters. The SNMP credentials are validated according to which SNMP version(s) are selected.

- If SNMP v1 Parameters or v2 Parameters is selected, enter the applicable community in the available text box.
- If SNMP v3 Parameters is selected, configure the following parameters:
  - Username
  - Auth. Type
  - Auth. Password
  - Privacy Type
  - Privacy Password

Note If SNMP v1 or v2 with default community is configured, the network is open to easy attacks because default communities are well known. SNMP v1 or v2 with a non-default community is more secure than a default community, but SNMP v3 with Auth and Privacy type and no default user is the most secure SNMP connection.

Step 11 Click **OK**.

If the NCS can use the SNMP credential listed to access the switch, the switch is added for later use and appears in the Configure > Ethernet Switches page.

Note If you manually added switches through the Configure > Ethernet Switches page, then switch port tracing uses the credentials from that page, not the ones listed in the SNMP Credentials page. If the manually-added switch credentials have changed, you need to update them from the Configure > Ethernet page.

Configuring SNMP Settings

The SNMP Settings page allows you to configure global SNMP settings from the NCS.

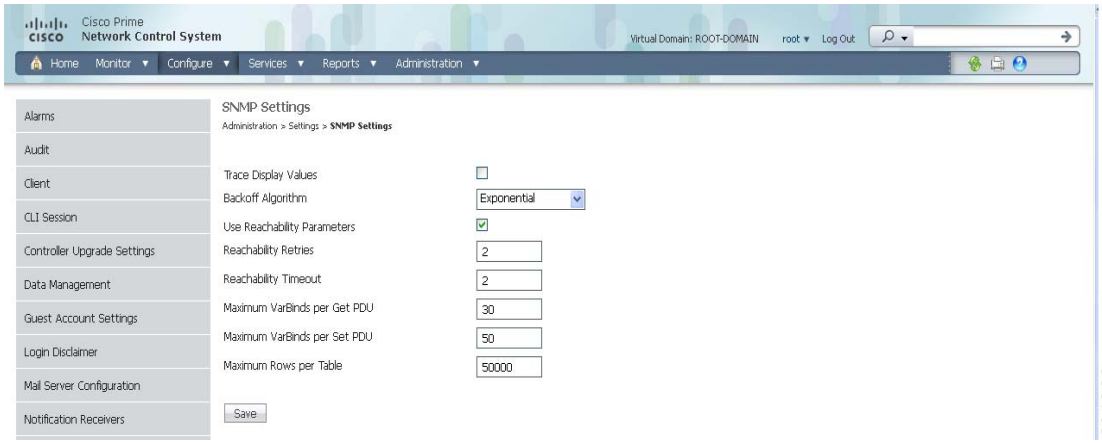
Note Any changes you make on this page affects the NCS globally. The changes are saved across restarts as well as across backups and restores.

To configure global SNMP settings, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **SNMP Settings**. The SNMP Settings page appears (see Figure 15-22).

Figure 15-22 SNMP Settings Page



Step 3 If the Trace Display Values check box is selected, mediation trace-level logging shows data values fetched from the controller using SNMP. If unselected, the values do not appear.

Note The default is unselected for security reasons.

Step 4 For the Backoff Algorithm, choose either **Exponential** or **Constant Timeout** from the drop-down list. If you choose Exponential (the default value), each SNMP try waits twice as long as the previous try, starting with the specified timeout for the first try. If you choose Constant Timeout, each SNMP try waits the same, specified amount of time.

Note Constant Timeout is useful on unreliable networks (such as satellite networks) where the desired number of retries is large. Because it does not double the timeout per try, it does not take as long to timeout with a high number of retries.

Step 5 Determine if you want to use reachability parameters. If selected, the NCS defaults to the global Reachability Retries and Timeout that you configure. If unselected, the NCS always uses the timeout and retries specified per-controller or per-IOS access point. The default is selected.

Note Adjust this setting downward if switch port tracing is taking a long time to complete.

Step 6 For the Reachability Retries field, enter the number of global retries used for determining device reachability. The default number is 2. This field is only available if the Use Reachability Parameters check box is selected.

Note Adjust this setting downward if switch port tracing is taking a long time to complete.

Step 7 For the Reachability Timeout field, enter a global timeout used for determining device reachability. The default number is 2. This field is only available if the Use Reachability Parameters check box is selected.

Step 8 At the Maximum VarBinds per PDU field, enter a number to indicate the largest number of SNMP variable bindings allowed in a request or response PDU. The default is 100.

Note For customers who have issues with PDU fragmentation in their network, this number can be reduced to 50, which typically eliminates the fragmentation.

Step 9 The maximum rows per table field is configurable and the default value is 50000 rows. The configured value is retained even if you upgrade the NCS version.

Step 10 Click **Save** to confirm these settings.

Configuring Switch Port Tracing

Currently, the NCS provides rogue access point detection by retrieving information from the controller. The rogue access point table is populated with any detected BSSID addresses from any frames that are not present in the neighbor list. At the end of a specified interval, the contents of the rogue table are sent to the controller in a CAPWAP Rogue AP Report message. With this method, the NCS simply gathers the information received from the controllers; but with software Release 5.1, you can now incorporate switch port tracing of Wired Rogue Access Point Switch Ports. This enhancement allows you to react to found wired rogue access points and prevent future attacks. The trace information is available only in the NCS log and only for rogue access points, not rogue clients.

Note Rogue Client connected to the Rogue Access point information is used to track the switch port to which the Rogue Access point is connected in the network.

Note If you try to set tracing for a friendly or deleted rogue, a warning message appears.

Note For Switch Port Tracing to successfully trace the switch ports using v3, all of the OIDs should be included in the SNMP v3 view and VLAN content should be created for each VLAN in the SNMP v3 group.

Note See the "Configuring Switch Port Tracing" section on page 15-77 for information on configuring Switch Port Tracing settings.

The Switch Port Trace page allows you to run a trace on detected rogue access points on the wire.

To correctly trace and contain rogue access points, you must correctly provide the following information.

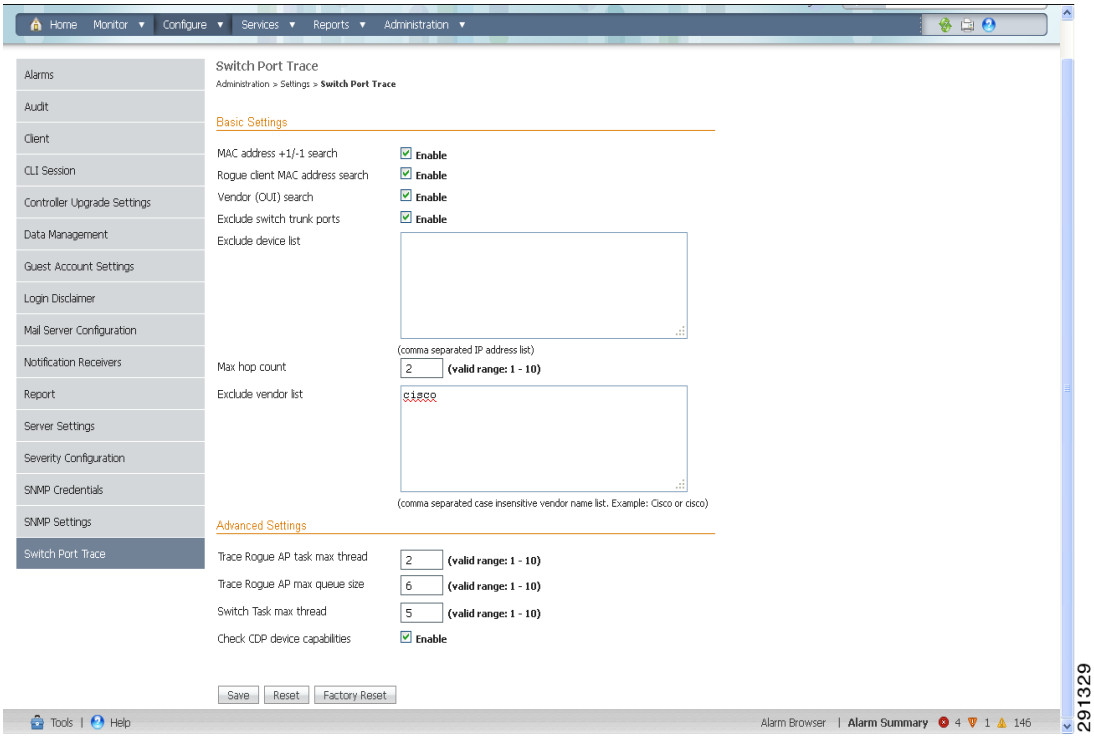
- Reporting APs—A rogue access point has to be reported by one or more managed access points.
- AP CDP Neighbor—Access point CDP neighbor information is required to determine the seed switches.
- Switch IP address and SNMP credentials—All switches to be traced must have a management IP address and SNMP management enabled. You can add network address based entries instead of only adding individual switches. The correct write community string must be specified to enable/disable switch ports. For tracing, read community strings are sufficient.
- Switch port configuration—Trunking switch ports must be correctly configured. Switch port security must be turned off.
- Only Cisco Ethernet switches are supported.
- Switch VLAN settings must be properly configured.
- CDP protocol must be enabled on all switches.
- An Ethernet connection must exist between the rogue access point and the Cisco switch.
- You should have some traffic between rogue access points and the Ethernet switch.
- The rogue access point must be connected to a switch within the max hop limit. The default hop count is 2, and the maximum is 10.
- If SNMPv3 is chosen, use the context option and create one for each VLAN, in addition to the one for the main group (which is required for non-VLAN-based MIBs).

To specify options for switch port tracing, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Switch Port Trace** (see Figure 15-23).

Figure 15-23 Switch Port Trace Page



Step 3 Configure the following basic settings as needed:

- MAC address +1/-1 search—Select the check box to enable.

  This search involves the MAC address +1/-1 convention where the wired-side MAC address of the rogue access point is obtained by adding or subtracting the radio MAC address by one.

- Rogue client MAC address search—Select the check box to enable.

  When a rogue access point client exists, the MAC address of the client is added to the searchable MAC address list.

- Vendor (OUI) search—Select the check box to enable. OUI refers to Organizational Unique Identifier search which searches the first 3 bytes in a MAC address.

- Exclude switch trunk ports—Select the check box to exclude switch trunk ports from the switch port trace.

  Note When more than one port is traced for a given MAC address, additional checks are performed to improve accuracy. These checks include: trunk port, non-AP CDP neighbors present on the port, and whether or not the MAC address is the only one on this port.

- Exclude device list—Select the check box to exclude additional devices from the trace. Enter into the device list text box each device that you want to exclude from the switch port trace. Separate each device names with commas.

- Max hop count—Enter the maximum number of hops for this trace. Keep in mind that the greater the hop count, the longer the switch port trace takes to perform.

- Exclude vendor list—Enter in the vendor list text box any vendors that you want to exclude from the switch port trace. Separate vendor names with commas. The vendor list is not case sensitive.

Step 4 Configure the following advanced settings as needed:

- TraceRogueAP task max thread—Switch port tracing uses multiple threads to trace rogue access points. This field indicates the maximum number of rogue access points that can be traced on parallel threads.
- TraceRogueAP max queue size—Switch port tracing maintains a queue to trace rogue access points. Whenever you select a rogue access point for tracing, it is queued for processing. This field indicates the maximum number of entries that you can store in the queue.
- SwitchTask max thread—Switch port tracing uses multiple threads to query switch devices. This field indicates the maximum number of switch devices that you can query on parallel threads.

Note The default value for these parameters should be good for normal operations. These parameters directly impact the performance of switch port tracing and NCS. Unless required, We do not recommend that you alter these parameters.

- Select CDP device capabilities—Select the check box to enable.

Note The NCS uses CDP to discover neighbors during tracing. When the neighbors are verified, the NCS uses the CDP capabilities field to determine whether or not the neighbor device is a valid switch. If the neighbor device is not a valid switch, it is not traced.

Step 5 Click **Save** to confirm changes made. Click **Reset** to return the page to the original settings. Click **Factory Reset** to return settings to the factory defaults.

Establishing Switch Port Tracing

To establish switch port tracing, follow these steps:

Step 1 In the NCS home page, click the **Security** dashboard.

Step 2 In the Rogue APs and Adhoc Rogues section, click the number URL which specifies the number of rogues in the last hour, last 24 hours, or total active.

Step 3 Choose for which rogue you are setting switch port tracking by clicking the URL in the MAC Address column. The Alarms > Rogue AP details page opens.

Step 4 From the Select a command drop-down list, choose **Trace Switch Port**. The Trace Switch Port page opens and NCS runs a switch port trace.

When one or more searchable MAC addresses are available, the NCS uses CDP to discover any switches connected up to two hops away from the detecting access point. The MIBs of each CDP discovered switch is examined to see if it contains any of the target MAC addresses. If any of the MAC addresses are found, the corresponding port number is returned and reported as the rogue switch port.

The SNMP communities for the switches are provided in the "Configuring Switches" section on page 8-200.

See the "Switch Port Tracing Details" section on page 15-81 for additional information on the Switch Port Tracing Details dialog box.

Switch Port Tracing Details

In the Switch Port Tracing Details dialog box, you can enable or disable switch ports, trace switch ports, and view detail status of the access point switch trace. For more information on Switch Port Tracing, see the following topics:

- Configuring Switch Port Tracing—Provides information on configuring switch port trace settings.
- Configuring Switches—Provides information on configuring SNMP switches.
- Configuring SNMP Credentials—Provides information on configuring SNMP switch credentials.

In the Switch Port tracing Details dialog box, do one of the following:

- Click **Enable/Disable Switch Port(s)**—Enables or disables any selected ports.
- Click **Trace Switch Port(s)**—Runs another switch port trace.
- Click **Show Detail Status**—Displays details regarding the switch port traces for this access point.
- Click **Close**.

Switch Port Tracing Troubleshooting

Switch Port Tracing (SPT) works on a best-effort-basis. SPT depends on the following information to correctly trace and contain rogue APs:

- Reporting access points—A rogue access point must be reported by one or more managed access points.
- Access point CDP neighbor—Access point CDP neighbor information is required to determine the seed switches.
- Switch IP address and SNMP credentials
  - All the switches that need to be traced should have a management IP address and SNMP management enabled.
  - With the new SNMP credential changes, instead of adding the individual switches to the NCS, network address based entries can be added.
  - The new SNMP credential feature has a default entry 0.0.0.0 with default community string as 'private' for both read/write.
  - Correct write community string has to be specified to enable/disable switch ports. For tracing, read community string should be sufficient.
- Switch port configuration
  - Switch ports that are trunking should be correctly configured as trunk ports.
  - Switch port security should be turned off.
- Only Cisco Ethernet switches are supported.

Note The following switches are supported: 3750, 3560, 3750E, 3560E, and 2960.

- Switch VLAN settings should be properly configured.
- CDP protocol should be enabled for all the switches.
- An Ethernet connection should exist between the rogue access point and the Cisco switch.
- There should be some traffic between the rogue access point and the Ethernet switch.
- The rogue access point should be connected to a switch within the max hop limit. Default hop is 2. Max hop is 10.
- If SNMPv3 is used, then make sure you use the context option and create one for each VLAN in addition to the one for the main group (which is required for non-VLAN based MIBs).

Setting User Preferences

Choose Administration > User Preferences to open the User Preferences page. The User Preferences page enables you to control certain display options in the NCS.

Note When the non-root users log into NCS and try to modify the user preferences, the "Permission Denied" message appears, which is an expected behavior.

List Pages

- Items Per List—You can set the number of items, such as controllers or access points, to display in pages that list these items. Choose the number of items to display from the Items Per List Page drop-down list.

User Idle Timeout

- Logout idle user—Select the check box if you want to configure the amount of time, in minutes, that a user session can be idle before the server cancels the session.
- Logout idle user after—Select the maximum number of minutes that a server waits for an idle user. The default value is 60 minutes. The minimum value is 15 minutes. The maximum value is 120 minutes.

Note If the Logout idle user check box is unselected, the user session does not time out.

Alarms

- Refresh Map/Alarms page on new alarm—Select the check box to refresh map and alarm pages each time a new alarm is generated.
- Refresh Alarm count in the Alarm Summary every—Choose the frequency of the Alarm Summary refresh from the drop-down list (every 5, seconds, 15 seconds, 30 seconds, 1 minute, 2 minutes, or 5 minutes).
- Display Alarm Category in Alarm Summary page—Choose the alarm category that you want to display in the minimized Alarm Summary (Alarm Summary, Malicious AP, Unclassified AP, Coverage Holes, Security, Controllers, Access Points, Mobility Services, Mesh Links, NCS, or Performance).

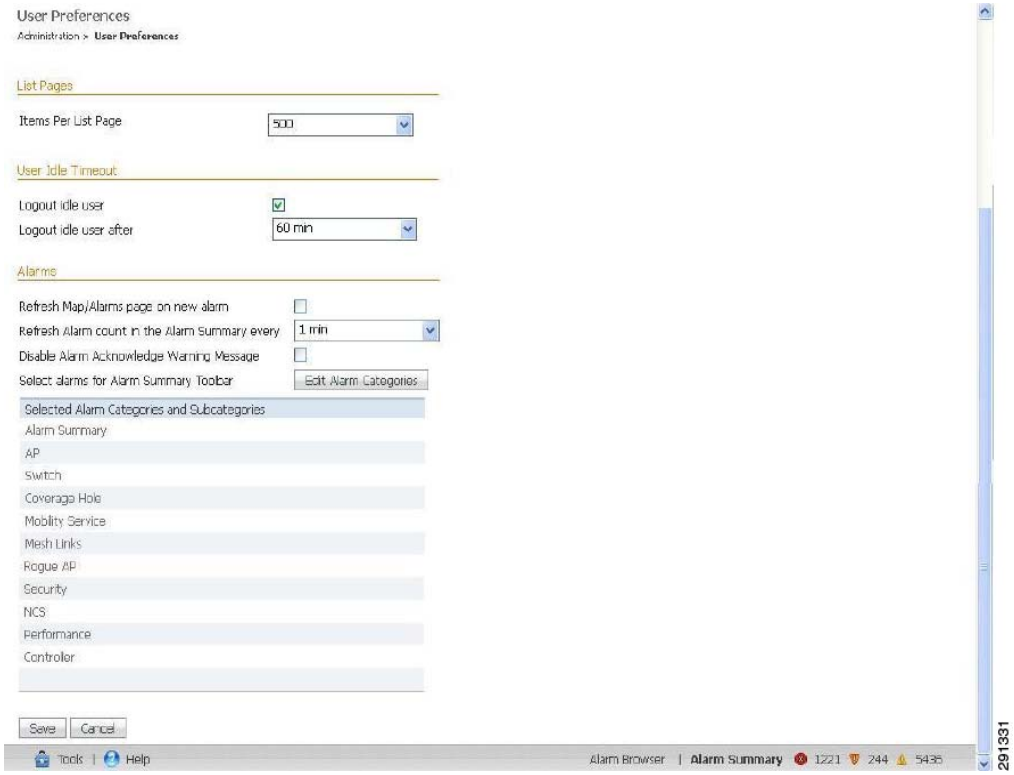
- Disable Alarm Acknowledge Warning Message—When you acknowledge an alarm, a warning displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Select this check box to stop the warning message from displaying.
- Select alarms for Alarm Summary Toolbar—To select alarms for the Alarm Summary Toolbar, click **Edit Alarm Categories** and choose the required alarm categories and subcategories.

This page contains user-specific settings you might want to adjust.

To change the user-specific settings, follow these steps:

Step 1 Choose **Administration > User Preferences**. The User Preferences Page appears (see Figure 15-24).

Figure 15-24 User Preferences Page



Step 2 Use the Items Per List Page drop-down list to configure the number of entries shown on a given list page (such as alarms, events, AP list, and so on).

Step 3 Specify how often you want the home page refreshed by selecting the **Refresh home page** check box and choosing a time interval from the Refresh home page every drop-down list.

Step 4 Select the **Logout idle user** check box and configure the Logout idle user after text box, in minutes, that a user session can be idle before the server cancels the session.

Step 5 If you want the maps and alarms page to automatically refresh when a new alarm is raised by the NCS, select the **Refresh Map/Alarms page on new alarm** check box in the Alarms portion of the page.

Step 6 From the Refresh Alarm count in the Alarm Summary every drop-down list choose a time interval to to specify how often to reset.

Step 7 If you do not want the alarm acknowledge warning message to appear, select the **Disable Alarm Acknowledge Warning Message** check box.

Step 8 Click **Edit Alarm Categories** to select the alarm categories to display in the Alarm Summary page.

Step 9 In the Select Alarms page, choose the default category to display from the drop-down list, and select the alarm categories and sub categories to display from the alarm toolbar. Click **Save** to save the alarm category list. The selected alarm category and sub categories appears in the User Preferences page.

Step 10 Click **Save** to save the User Preference settings.

Viewing Appliance Details

This section provides the Appliance details. This section contains the following topics:

Viewing Appliance Status Details

To view the appliance status, perform the following steps:

Step 1 Choose **Administration > Appliance**.

Step 2 Choose **Appliance Status** from the left sidebar menu. The Appliance Status page appears (see Figure 15-25) with the following details, see Table 15-5 for more information.

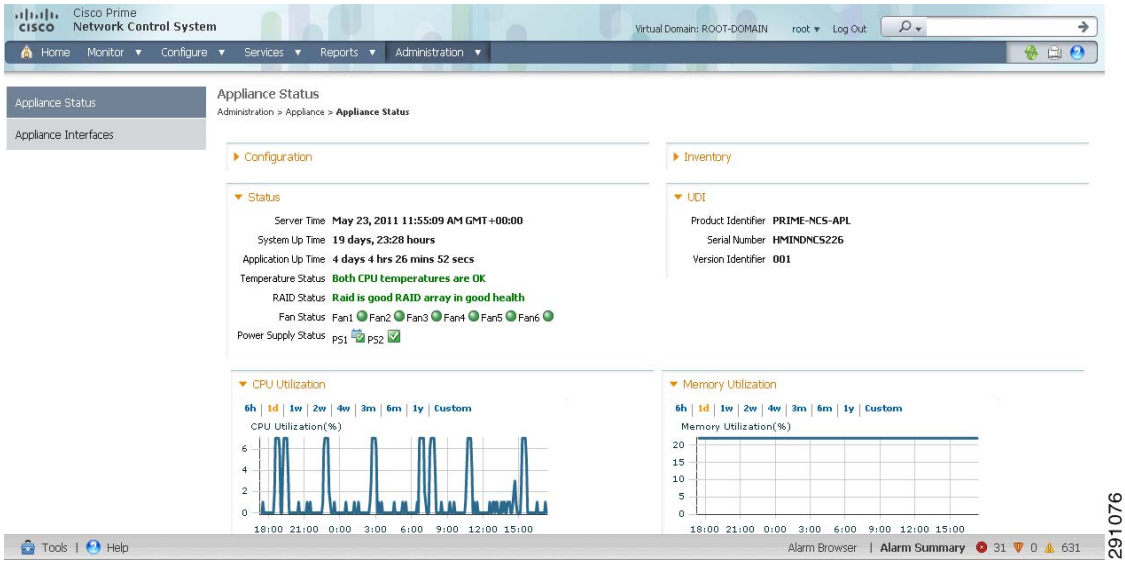
Table 15-5 Appliance Status Details

Field	Description
Configure Details	
Host Name	The hostname of the machine. If the hostname of the user machine is not in DNS, the IP address is displayed.
Domain Name	Domain Name of the server.
Default Gateway	IP address of the default gateway for the network environment in which you belong.
DNS Server(s)	Enter the IP address of the DNS server(s). Each DNS server must be able to update a client DNS entry to match the IP address assigned by this DHCP scope.
NTP Host(s)	Enter the IP address of the NTP server(s).
Status Details	
Server Time	The System time of the server.
System Up Time	It is a measure of the time since the server has been up without any downtime.

Table 15-5 Appliance Status Details (continued)

Field	Description
Application Up Time	It is a measure of the time since the NCS has been up without any downtime.
Temperature Status	The temperature status of the server.
RAID Status	The RAID status of the server.
Fan Status	The status of the cooler fans of the server.
Power Supply Status	The status of the power supply units of the server.
CPU Utilization	CPU Utilization of the server.
Memory Utilization	Memory Utilization of the server.
Inventory Details	Detailed inventory report.
UDI Details	
Product Identifier	The Product ID identifies the type of device.
Serial Number	The Serial Number is an 11 digit number which uniquely identifies a device.
Version Identifier	The VID is the version of the product. Whenever a product has been revised, the VID is incremented.

Figure 15-25 Appliance Status Page



Viewing Appliance Interface Details

To view the Appliance Interface details, follow these steps:

Step 1 Choose **Administration > Appliance**.

Step 2 Choose **Appliance Interface** from the left sidebar menu. The Interfaces page appears (see Figure 15-26).

Figure 15-26 Appliance Interface Details

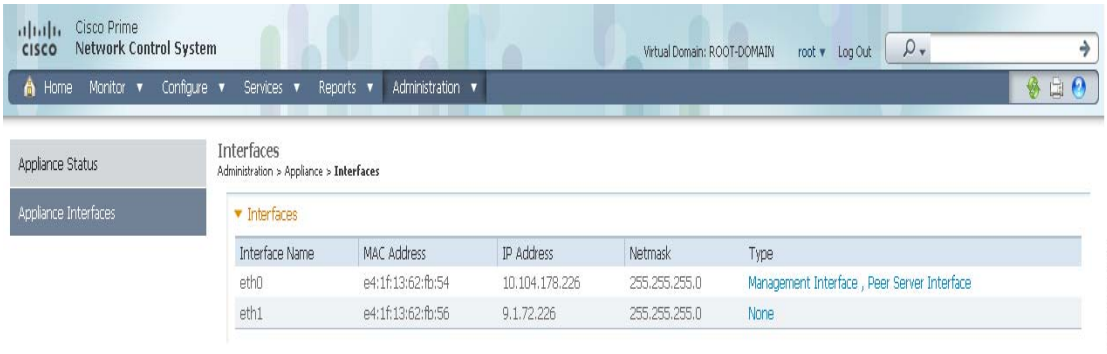


Table 15-6 Appliance Interface Details

Field	Description
Interface Name	User-defined name for this interface.
MAC Address	MAC address of the interface.
IP Address	Local network IP address of the interface.
Netmask	A range of IP addresses defined so that only machines with IP addresses within the range are allowed to access an Internet service.
Type	Static (Management, Peer, AP-Manager, Service-Port, and Virtual interfaces) or Dynamic (operator-defined interfaces).

Step 3 Click the **Interface Type** to configure if the interface belongs to peer server or to the management interfaces.

Configuring AAA

This section contains the following topics:

Configuring AAA Using the NCS

From Administration > AAA, authentication, authorization, and accounting (AAA) can be configured for the NCS. The only username that has permissions to configure NCS AAA is *root* or SuperUser. Any changes to local users accounts are in effect when configured for local mode. If using external authentication, for example RADIUS or TACACS+, the user changes must be done on the remote server.

This section contains the following topics:

Changing Password

Choose **Administration > AAA > Change Password** from the left sidebar menu to access this page.

This page enables you to change the password for current logged in User.

- User—Applies to the logged in User.
- Old Password—Current password.
- New Password—Enter the new password using ASCII characters.
- Confirm password—Reenter the new password.
- Submit—Click **Submit** to confirm password change.

Configuring AAA Mode

Choose **Administration > AAA > AAA Mode** from the left sidebar menu to access this page.

This page enables you to configure the authentication mode for all users.

- AAA Mode Settings
  - Local—Authenticate users to a local database.
  - RADIUS—Authenticate users to an external RADIUS server.
  - TACACS+—Authenticate users to an external TACACS+ server.
- Enable fallback to Local—If an external authentication server is down, this provides the option to authenticate users locally. This check box is only available for RADIUS and TACACS+.
  - Choose **ONLY on no server response** or **on auth failure or no server response** from the drop-down list.

See also the "Configuring TACACS+ Servers" section on page 15-95 and the "Configuring RADIUS Servers" section on page 15-98.

AAA Mode Settings

To choose a AAA mode, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 Choose **AAA Mode** from the left sidebar menu. The AAA Mode Settings page appears (see Figure 15-27).

Figure 15-27 AAA Mode Settings Page

Step 3 Choose which AAA mode you want to use. Only one can be selected at a time.

Any changes to local user accounts are effective only when you are configured for local mode (the default). If you use remote authentication, changes to the credentials are made on a remote server. The two remote authentication types are RADIUS and TACACS+. RADIUS requires separate credentials for different locations (East and West Coast). TACACS+ is an effective and secure management framework with a built-in failover mechanism.

Step 4 Select the **Enable Fallback to Local** check box if you want the administrator to use the local database when the external AAA server is down.

Note This check box is unavailable if *Local* was selected as a AAA mode type.

Step 5 Click **OK**.

Configuring Local Password Policy

Choose **Administration > AAA > Local Password Policy** from the left sidebar menu to access this page.This page enables you to determine your local password policy.

You can enable or disable the following policies for your local password:

- Set the minimum length of your password. By default it is set as 8.
- Password cannot be the username or the reverse of the username.
- Password cannot be the word cisco or ocsic (cisco reversed) or any special characters replaced for the same.

- Root password cannot be the word public.
- No character can be repeated more than three time consecutively in the password.
- Password must contain character from three of the character classes: upper case, lower case, digits, and special characters.

Click **Save** to confirm the Local Password Policy changes.

Configuring Users

This section describes how to configure an NCS user. Besides complete access, you can give administrative access with differentiated privileges to certain user groups.

Choose **Administration > AAA > Users** from the left sidebar menu to access this page. You can use this page to view the User details, create a User, delete a User as well as edit User details.

This section contains the following topics:

Viewing User Details

You can view the NCS user details in the Users page. The following information is available in the Administration > AAA > Users page:

- Current User Names
- Member Of—Groups with which the user is associated. Click an item in the Member Of column to view permitted tasks for this user.
- Audit Trail—Click the Audit Trail icon for a specific user to view or clear current audit trails. See the "Audit User Operations" section on page 15-92.

Note The NCS supports a maximum of 25 concurrent User logins at any point in time.

Edit Current Users - Passwords and Assigned Groups

To edit current user account passwords and assigned groups, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 Select a specific user from the User Name column.

Step 4 (Optional) Enter and confirm a new password, if necessary.

Step 5 If necessary, make changes to the Groups Assigned to this User check box selections.

Note If the user belongs to Lobby Ambassador, Monitor Lite, North Bound API, or User Assistant group, the user cannot belong to any other group.

Step 6 Select **Submit** to confirm the changes or **Cancel** to close the page without activating any changes.

Edit Current Users - Permitted Tasks

To edit the permitted tasks for this user account, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 Select the applicable group(s) from the Member Of column.

Step 4 From the List of Tasks Permitted column, select or deselect the applicable tasks to permit or disallow them.

Note The list of available tasks changes depending on the type of group.

Step 5 Select **Submit** to confirm the changes or **Cancel** to close the page without activating any changes.

Edit Current Users - Groups Assigned to this User

To edit the groups assigned to this user, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 Select a specific user from the User Name column.

Step 4 Select the check box(es) of the groups to which this user is assigned.

Note If the user belongs to Lobby Ambassador, Monitor Lite, North Bound API, or User Assistant group, the user cannot belong to any other group.
Root is only assignable to 'root' user and that assignment cannot be changed.

Note For more information on assigned groups, see Step 7 in the "Adding a New User" section on page 15-91 section.

Step 5 Select **Submit** to confirm the changes or **Cancel** to close the page without activating any changes.

Adding a New User

The Add User page allows the administrator to set up a new user login including username, password, groups assigned to the user, and virtual domains for the user. For more information on assigning virtual domains, see the "Assign a Virtual Domain" section on page 15-92.

Note By assigning virtual domains to a user, the user is restricted to information applicable to those virtual domains.

Note You must have SuperUser status to access this page.

Add User Name, Password, and Groups

To add a new user, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 From the Select a command drop-down list, choose **Add User**.

Step 4 Click **Go**.

Step 5 Enter a new username.

Step 6 Enter and confirm a password for this account.

Step 7 Select the check box(es) of the groups to which this user is assigned.

Note If the user belongs to Lobby Ambassador, Monitor Lite, North Bound API, or User Assistant group, the user cannot belong to any other group.

- Admin—Allows users to monitor and configure NCS operations and perform all system administration tasks except administering NCS user accounts and passwords.
- Config Managers—Allows users to monitor and configure NCS operations.
- Lobby Ambassador—Allows guest access for configuration and management only of user accounts. If Lobby Ambassador is selected, a Lobby Ambassador Defaults tab appears. See the "Managing Lobby Ambassador Accounts" section on page 6-17 for more information on setting up a Lobby Ambassador account.
- Monitor Lite—Allows monitoring of assets location.
- North Bound API User—Group used only with NCS Web Service consumers.

Note North Bound API Users cannot be assigned a virtual domain. When a North Bound API group is selected, the Virtual Domains tab is not available.

Note You can add a North Bound API User only if you are logged into the ROOT-DOMAIN.

- Root—This group is only assignable to 'root' user and that assignment cannot be changed.

- Super Users—Allows users to monitor and configure NCS operations and perform all system administration tasks including administering NCS user accounts and passwords. Superuser tasks can be changed.
- System Monitoring—Allows users to monitor NCS operations.
- User Assistant—Allows local net user administration only.
- User Defined.

Assign a Virtual Domain

To assign a virtual domain to this user, follow these steps:

Step 1 Select the **Virtual Domains** tab. This page displays all virtual domains available and assigned to this user.

Note The Virtual Domains tab enables the administrator to assign virtual domains for each user. By assigning virtual domains to a user, the user is restricted to information applicable to those virtual domains.

Note North Bound API Users cannot be assigned a virtual domain. When a North Bound API group is selected, the Virtual Domains tab is not available.

Step 2 Click to highlight the virtual domain in the Available Virtual Domains list that you want to assign to this user.

Note You can select more than one virtual domain by pressing the Shift or Control key.

Step 3 Click **Add**. The virtual domain moves from the Available Virtual Domains to the Selected Virtual Domains list.

To remove a virtual domain from the Selected Virtual Domains list, click to highlight the domain in the Selected Virtual Domains list and click **Remove**. The virtual domain moves from the Selected Virtual Domains to the Available Virtual Domains list.

Step 4 Select **Submit** or **Cancel** to close the page without adding or editing the current user.

Audit User Operations

To view or clear audit information for this account, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 Click the **Audit Trail** icon for the applicable account.

Note You must have SuperUser status to access this page.

This page enables you to view a list of user operations over time.

- User—User login name.
- Operation—Type of operation audited.
- Time—Time operation was audited.
- Status—Success or Failure.
- Reason—Reason is applicable only for failure.
- Configuration Changes—This field provides a Details link if there are any configuration changes. Click the Details link for more information on the configuration changes done by an individual user. The entries list out the change of values for individual parameters between the NCS and controller. For more information on Audit Trail Details, see the "Audit Trail Details Page" section on page 6-10.

Step 4 To clear an audit trail, select the check box for the applicable audit, select Clear Audit Trail from the Select a command drop-down list, click **Go**, and click **OK** to confirm.

Configuring Groups

This page provides you with a list of all current groups and their associated members.

- Group Name—Click a specific group to view or edit the permitted tasks for this group. The available tasks change depending on the type of group. See the "Edit Current Users - Permitted Tasks" section on page 15-90 for more information.
- Members—Click a specific user under the Member column to view or edit that user. See the "Edit Current Users - Passwords and Assigned Groups" section on page 15-89 for more information.
- Audit Trail—Click the Audit Trail icon to view or clear audit for this group. See the "Audit User Operations" section on page 15-92 for more information.
- Export—Click to export the task list associated with this group.

To access the Groups page, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **User Group**.

Note You must have SuperUser status to access this page.

Viewing or Editing User Group Information

To see specific tasks the user is permitted to do within the defined group or make changes to the tasks, follow these steps:

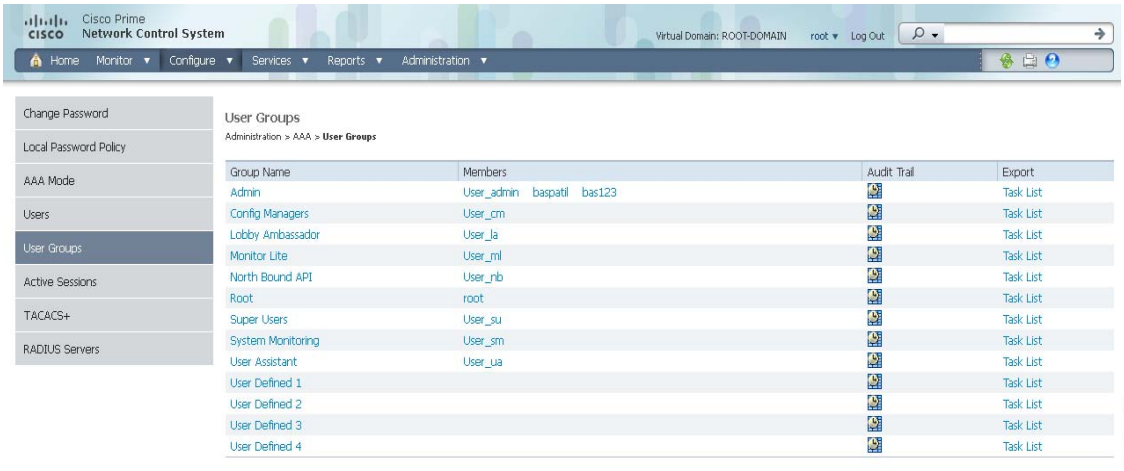
Step 1 Choose **Administration > AAA**.

Step 2 Choose **User Groups** from the left sidebar menu.

Step 3 Click in the **Group Name** column. The Group Detail: *User Group* page appears (see Figure 15-28).

Note The detailed page varies based on what group you choose. Figure 15-28 shows the detailed page of the superuser.

Figure 15-28 Detailed User Groups Page



You can see the specific tasks the user is permitted to do within the defined group.

Step 4 Click Audit Trail to view the audit trail information for the corresponding User group. For more information on Audit Trail Details, see the "Audit Trail Details Page" section on page 6-10.

Step 5 Make any necessary changes to the tasks.

Table 15-7 Default User Groups

User Group	Description
Admin	Group for NCS Administration.
Config Managers	Group for monitoring and configuration tasks.
Lobby Ambassador	Group to allow Guest user administration only. This Group is not editable.
Monitor Lite	Group to allow monitoring of assets only. Group is not editable.
North Bound API	Group to allow access to North Bound APIs. Group is not editable.
Root	Group for root user. Group is not editable.
Super Users	Group to allow all NCS tasks.
System Monitoring	Group for monitoring only tasks.
User Assistant	Group to allow Local Net user administration only. Group is not editable.
User-Defined 1	User definable group.
User-Defined 2	User definable group.
User-Defined 3	User definable group.
User-Defined 4	User definable group.

Step 6 Click **Submit**.

Viewing Active Sessions

Choose **Administration > AAA > Active Sessions** from the left sidebar menu to open this page.

This page displays a list of users currently logged in. The user highlighted in red represents your current login.

Note You must be logged into a user account with SuperUsers privileges to see active sessions.

If a column heading is a hyperlink, click the heading to sort the list of active sessions in descending or ascending order along that column. The sort direction is toggled each time the hyperlink is clicked.

The Active Sessions page has the following columns:

- Username—The User ID of the User who is logged in.
- IP/Host Name—The IP address or the hostname of the machine on which the browser is running. If the hostname of the user machine is not in DNS, the IP address is displayed.
- Login Time—The time at which the user logged in to the NCS. All times are based on the NCS server machine time.
- Last Access Time—The time at which the user browser accessed the NCS. All times are based on the NCS server machine time.

  Note The time displayed in this column is usually a few seconds behind the current system time because Last Access Time is updated frequently by the updates to the alarm status panel. However, if a user navigates to a non-NCS web page in the same browser, the disparity in time is greater. Alarm counts are not updated when the browser is not displaying NCS web pages.

- Login Method—The login method can be any of the following:
  - Local
  - Radius
  - TACACS+
- User Groups—The list of groups the user belongs to.
- Audit trail icon—Link to page that displays the audit trail (previous login times) for that user.

Configuring TACACS+ Servers

This section describes how to add and delete TACACS+ servers. TACACS+ servers provide an effective and secure management framework with built-in failover mechanisms. If you want to make configuration changes, you must be authenticated.

The TACACS+ page shows the IP address, port, retransmit rate, and authentication type (Password Authentication Protocol (PAP)) or Challenge Handshake Authentication Protocol (CHAP) of the TACACS+ server. The TACACS+ servers are tried based on how they were configured.

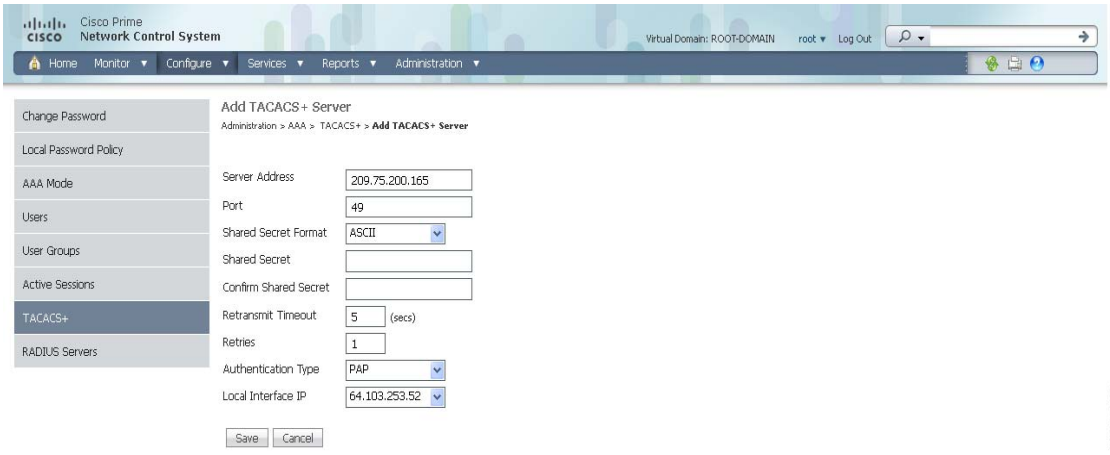
Note To activate TACACS+ servers, you must enable them as described in the "Configuring ACS 4.x" section on page 15-103.

To configure TACACS+, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **TACACS+**. The TACACS+ page appears (see Figure 15-29).

Figure 15-29 TACACS+ Page



Step 3 The TACACS+ page shows the IP address, port, retransmit rate, and authentication type (Password Authentication Protocol (PAP)) or Challenge Handshake Authentication Protocol (CHAP) TACACS+ server. The TACACS+ servers are tried based on how they were configured.

Note If you need to change the order of how TACACS+ servers are tried, delete any irrelevant TACACS+ servers and readd the desired ones in the preferred order.

Step 4 Use the drop-down list in the upper right-hand corner to add or delete TACACS+ servers. You can click an IP address if you want to make changes to the information.

Step 5 The current server address and port are displayed. Use the drop-down list to choose either ASCII or hex shared secret format.

Step 6 Enter the TACACS+ shared secret used by your specified server.

Step 7 Reenter the shared secret in the Confirm Shared Secret text box.

Step 8 Specify the time in seconds after which the TACACS+ authentication request times out and a retransmission is attempted by the controller.

Step 9 Specify the number of retries that are attempted.

Step 10 In the Authentication Type drop-down list, choose PAP or CHAP protocol.

Step 11 In the Local Interface IP drop-down list, choose an IP address for the interface.

This interface IP address is the same that you specify in the ACS Server for TACACS+.

Step 12 Click **Submit**.

Note The RADIUS/TACACS server IP address and other credentials created in the 7.0.x releases are not migrated to NCS 1.0. You need to add them again after the migration from 7.0.x to NCS 1.0 is complete.

Note See the "Configuring ACS 5.x" section on page 15-113 for more information on Configuring ACS 5.x.

Select a command

- Add TACACS+ Server—See the "Add TACACS+ Server" section on page 15-97.
- Delete TACACS+ Server—Select a server or servers to be deleted, select this command, and click **Go** to delete the server(s) from the database.

Add TACACS+ Server

Choose **Administration > AAA > TACACS+** from the left sidebar menu to access this page. From the Select a command drop-down list choose **Add TACACS+ Server**, and click **Go** to access this page.

This page allows you to add a new TACACS+ server to the NCS.

- Server Address—IP address of the TACACS+ server being added.
- Port—Controller port.
- Shared Secret Format—ASCII or Hex.
- Shared Secret—The shared secret that acts as a password to log in to the TACACS+ server.
- Confirm Shared Secret—Reenter TACACS+ server shared secret.
- Retransmit Timeout—Specify retransmission timeout value for a TACACS+ authentication request.
- Retries—Number of retries allowed for authentication request. You can specify a value between 1 and 9.
- Authentication Type—Two authentication protocols are provided. Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

Command Buttons

- Submit
- Cancel

Note

- Enable the TACACS+ server with the AAA Mode Settings. See the "Configuring AAA Mode" section on page 15-87.
- You can add only three servers at a time in the NCS.

Configuring RADIUS Servers

This section describes how to add and delete RADIUS servers. You must enable RADIUS servers and have a template set up for them to make configuration changes.

RADIUS provides authentication of users accessing the network. Authentication requests are sent to a RADIUS server that contains all user authentication and network access information. Passwords are encrypted using RADIUS.

In the event the configured RADIUS server(s) is down, NCS falls back to local authentication and authorization if the fallback to local option is configured. See the "Configuring AAA Mode" section on page 15-87.

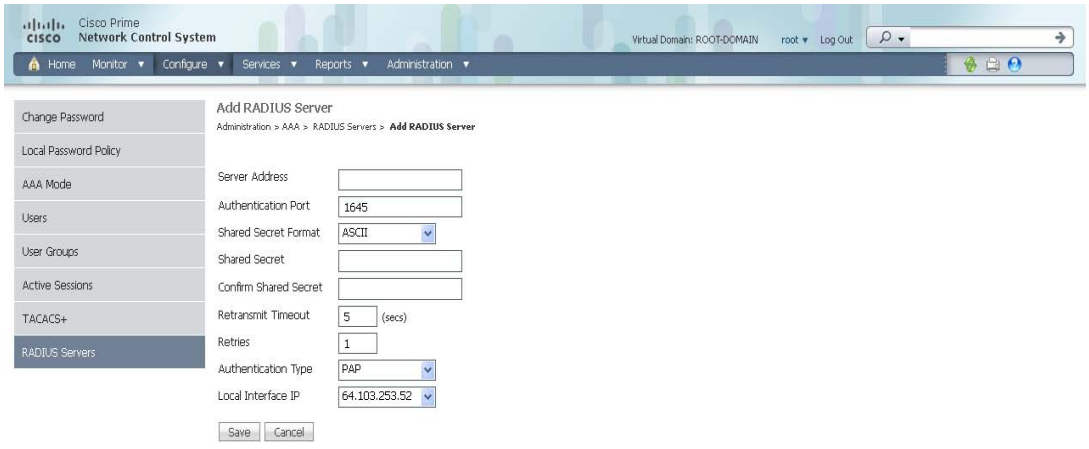
Note To activate RADIUS servers, you must enable them as described in the "Configuring ACS 4.x" section on page 15-103.

To configure a RADIUS server, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **RADIUS**. The RADIUS page appears (see Figure 15-30).

Figure 15-30 RADIUS Page



Step 3 The RADIUS page shows the server address, authentication port, retransmit timeout value, and authentication type for each RADIUS server that is configured. The RADIUS servers are tried based on how they were configured.

Note If you need to change the order of how RADIUS servers are tried, delete any irrelevant RADIUS servers, and readd the desired ones in the preferred order.

Step 4 Use the drop-down list in the upper right-hand corner to add or delete RADIUS servers. You can click an IP address if you want to make changes to the information.

Step 5 The current authentication port appears. Use the drop-down list to choose either ASCII or hex shared secret format.

Step 6 Enter the RADIUS shared secret used by your specified server.

Step 7 Reenter the shared secret in the Confirm Shared Secret text box.

Step 8 Specify the time in seconds after which the RADIUS authentication request times out and a retransmission is attempted by the controller.

Step 9 Specify the number of retries that are attempted.

Step 10 From the Authentication Type drop-down list, choose PAP or CHAP protocol.

Step 11 In the Local Interface IP drop-down list, choose an IP address for the interface.

This interface IP address is the same that you specify in the ACS Server for RADIUS.

Step 12 Click **Submit**.

Select a command

- Add RADIUS Server—See the "Adding RADIUS Server" section on page 15-99.
- Delete RADIUS Server—Select a server or servers to be deleted, select this command, and click **Go** to delete the server(s) from the database.

Adding RADIUS Server

Choose **Administration > AAA > RADIUS** from the left sidebar menu to access this page. From the Select a command drop-down list choose **Add RADIUS Server**, and click **Go** to access this page.

This page allows you to add a new RADIUS server to the NCS.

- Server Address—IP address of the RADIUS server being added.
- Port—Controller port.
- Shared Secret Format—ASCII or Hex.
- Shared Secret—The shared secret that acts as a password to log in to the RADIUS server.
- Confirm Shared Secret—Reenter the RADIUS server shared secret.
- Retransmit Timeout—Specify the retransmission timeout value for a RADIUS authentication request.
- Retries—Number of retries allowed for authentication request. You can specify a value between 1 to 9.

Command Buttons

- Submit
- Cancel

Note

- Enable the RADIUS server with the AAA Mode Settings. See the "Configuring AAA Mode" section on page 15-87.
- You can add only three servers at a time in the NCS.

Authenticating AAA Users Through RADIUS Using Cisco Identity Services Engine (ISE)

You can integrate an NCS with ISE. This section explains the NCS user authentication through Radius protocol using ISE.

This authentication helps you in setting up Users in ISE who are configured locally and not from external sources such as Active Directory and LDAP.

Note Only RADIUS server authentication is supported in ISE.

To authenticate AAA through RADIUS server using ISE, following steps:

Step 1 Add the NCS as a AAA client in ISE. For more information, see the "Adding the NCS as a AAA client in ISE" section on page 15-100.

Step 2 Create a new User group in ISE. For more information, see the "Creating a New User Group in ISE" section on page 15-101.

Step 3 Create a new User in ISE and add that User to the User group created in ISE. For more information, see the "Creating a New User and Adding to a User Group in ISE" section on page 15-101.

Step 4 Create a new Authorization profile. For more information, see the "Creating a New Authorization Profile in ISE" section on page 15-101.

Step 5 Create an Authorization policy rule. For more information, see the "Creating an Authorization Policy Rule in ISE" section on page 15-102.

Step 6 Configure AAA in the NCS. For more information, see the "Configuring AAA in the NCS" section on page 15-103.

Adding the NCS as a AAA client in ISE

To add NCS as a AAA client in ISE, follow these steps:

Step 1 Log in to ISE.

Step 2 Choose **Administration > Network Devices**.

Step 3 From the left sidebar menu, click the arrow next to Network Devices to expand that option.

The expanded list shows the already added devices.

Step 4 Click any device to view its details.

Step 5 From the left sidebar menu, click the arrow next to the  icon, and choose the **Add new device** option.

Step 6 In the right pane, enter the following details for the device you want to add:

- Name—Name of the device.
- Description—Device description.
- IP Address—NCS server IP address. For example, enter `209.165.200.225`.

Step 7 Enter the Shared key in the Shared Secret text box.

Click **Save** to add the device.

Creating a New User Group in ISE

You can create a new user group in ISE. This helps you to classify different privileged NCS users and also create authorization policy rules on user groups.

To create a new user group in ISE, follow these steps:

Step 1 Choose **ISE > Administration > Groups**.

Step 2 From the left sidebar menu, choose **User Identity Groups**.

The User Identity Groups page appears in the right pane.

Step 3 Click **Add**.

The Identity Group details page appears.

Step 4 Enter the name and description for the group.

For example, create a user group *NCS-SystemMonitoring-Group*.

Step 5 Click **Save**.

Creating a New User and Adding to a User Group in ISE

You can create a new user in ISE and map that user to a user group.

To create a new user and map that user to a user group in ISE, follow these steps:

Step 1 Choose **ISE > Administration > Identity Management > Identities**.

Step 2 From the left sidebar menu, choose **Identities > Users**.

The Network Access Users page appears in the right pane.

Step 3 Click **Add**.

The Network Access User page appears.

Step 4 Enter the Username, password and reenter password for the user.

For example, create a User *ncs-sysmon*.

Step 5 Choose the required user group from the **User Group** drop-down list, and click **Save**.

The new user is added to the required user group.

Note You can also integrate ISE with external sources such as Active Directory and LDAP.

Creating a New Authorization Profile in ISE

You can create authorization profiles in ISE. To create a new authorization profile, follow these steps:

Step 1 Choose **ISE > Policy > Policy Elements > Results**.

Step 2 From the left sidebar menu, choose **Authorization > Authorization Profiles**.

The Standard Authorization Profiles page appears in the right pane.

Step 3 Click **Add**.

The details page appears.

Step 4 Enter the name and description for the profile.

For example, create an authorization profile named *NCS-SystemMonitor*.

Step 5 Choose **ACCESS_ACCEPT** from the Access Type drop-down list.

Step 6 In the Advanced Attribute Settings group box, add the NCS User Group Radius Custom attributes one after another along with virtual domain attributes at the end. Select **cisco - av - pair** and paste the NCS User Group Radius custom attribute next to it. Keep adding one after another. Repeat the same step for virtual domain attributes as well.

Step 7 Save the authorization profile.

Creating an Authorization Policy Rule in ISE

To create an authorization policy rule, follow these steps:

Step 1 Choose **ISE > Policy > Authorization**.

Step 2 From the Authorization Policy page, choose **Insert New Rule Above** from the Actions drop-down list.

Create a rule which would be used for NCS user login.

Step 3 Enter a name for the rule in the Rule Name text box.

Step 4 Choose the required identity group from the Identity Groups drop-down list.

For Example, choose **NCS-SystemMonitoring-Group**.

For more information on creating Identity User Groups, see the "Creating a New User Group in ISE" section on page 15-101.

Step 5 Choose a permission from the Permissions drop-down list. The permissions are the Authorization profiles.

For Example, choose **NCS-SystemMonitor authorization profile**.

For more information on creating authorization profiles, see the "Creating a New Authorization Profile in ISE" section on page 15-101.

In this example, we define a rule where all users belonging to the NCS System Monitoring Identity Group receive an appropriate authorization policy with system monitoring custom attributes defined.

Step 6 Click **Save** to save the authorization rule.

Note You can also monitor successful and failed authentication using the ISE > Monitor > Authentications option.

Configuring AAA in the NCS

To configure AAA in the NCS, follow these steps:

Step 1 Log in to NCS as *root*.

Step 2 Choose **NCS > Administration > AAA > RADIUS Servers**.

Step 3 Add a new RADIUS Server with the ISE IP address.

For example, enter `209.165.200.230`.

Step 4 Click **Save** to save the changes.

Step 5 Choose **ISE > Administration > AAA > AAA Mode Settings**.

The AAA Mode Settings page appears.

Step 6 Select **RADIUS** as the AAA mode.

Step 7 Click **Save**.

The AAA mode is set to RADIUS in the NCS.

Step 8 Log out of the NCS.

Step 9 Log in again to the NCS as a AAA user, defined in ISE.

For example, log in as user *ncs-sysmon*.

For more information on creating users in ISE, see the "Creating a New User and Adding to a User Group in ISE" section on page 15-101.

Configuring ACS 4.x

This section provides instructions for configuring ACS 4.x to work with the NCS.

To import tasks into Cisco Secure ACS server, you must add the NCS to an ACS server (or non-Cisco ACS server). This section contains the following topics:

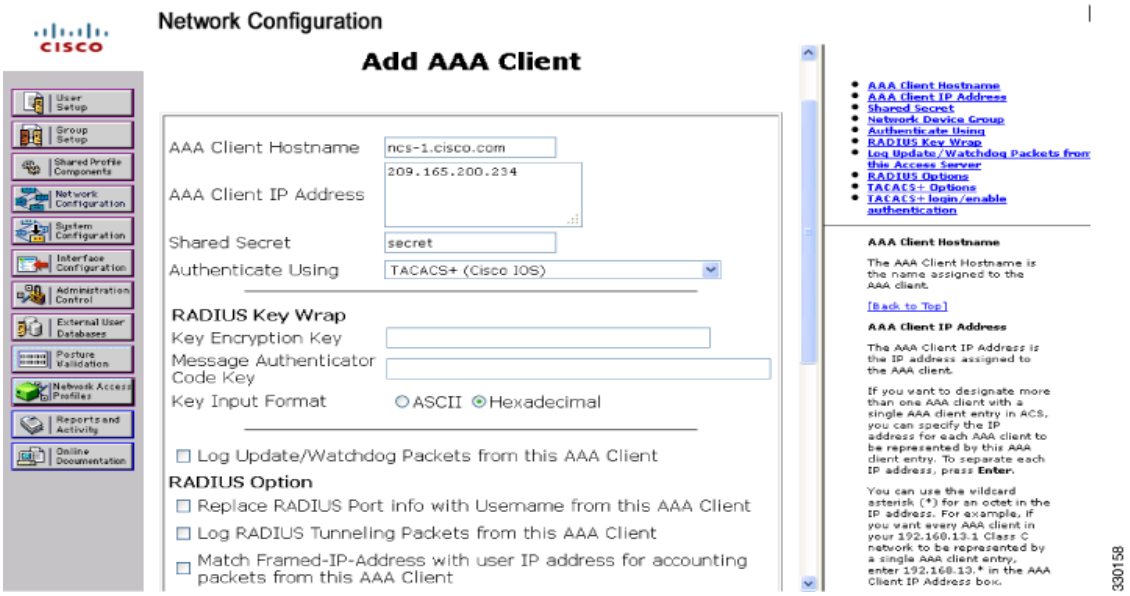
Adding the NCS to an ACS Server for Use with TACACS+ Server

To add the NCS to a TACACS+ server, follow these steps:

Note The instructions and illustrations in this section pertain to ACS Version 4.1 and might vary slightly for other versions or other vendor types. See the CiscoSecure ACS documentation or the documentation for the vendor you are using.

Step 1 Click **Add Entry** in the Network Configuration page of the ACS server (see Figure 15-32).

Figure 15-31 ACS Server Network Configuration Page



Step 2 In the AAA Client Hostname text box, enter the NCS hostname.

Step 3 Enter the NCS IP address in the AAA Client IP Address text box.

Ensure the interface that you use for ACS is the same as that is specified in the NCS and it is reacheable.

Step 4 In the Shared Secret text box, enter the shared secret that you want to configure on both the NCS and ACS servers.

Step 5 Choose **TACACS+** in the Authenticate Using drop-down list.

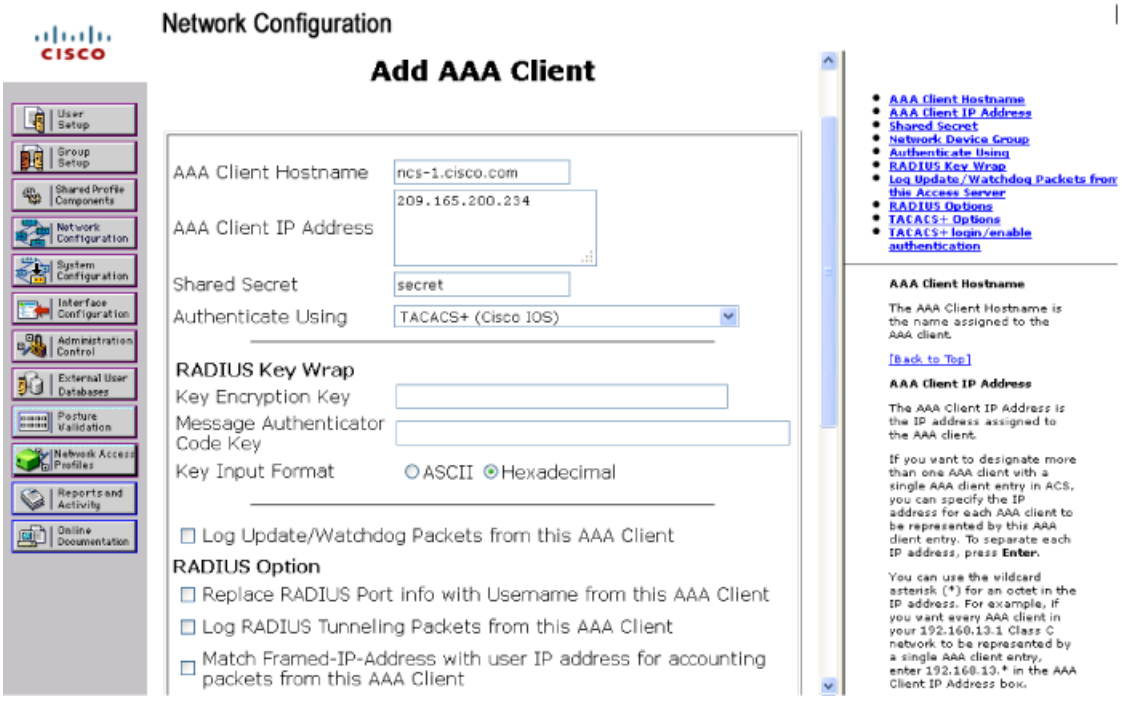
Step 6 Click **Submit + Apply**.

Step 7 From the left sidebar menu, choose **Interface Configuration**.

Step 8 In the Interface Configuration page, click the **TACACS+ (Cisco IOS)** link.

The TACACS+ (Cisco IOS) Interface Configuration page appears (see Figure 15-32).

Figure 15-32 ACS Server Network Configuration Page



Step 9 In the New Services portion of the page, add **NCS** in the Service column heading.

Step 10 Enter **HTTP** in the Protocol column heading.

Note HTTP must be in uppercase.

Step 11 Select the check box in front of these entries to enable the new service and protocol.

Note The ACS 4.x configuration is complete only when you specify and enable the NCS service with HTTP protocol.

Step 12 Click **Submit**.

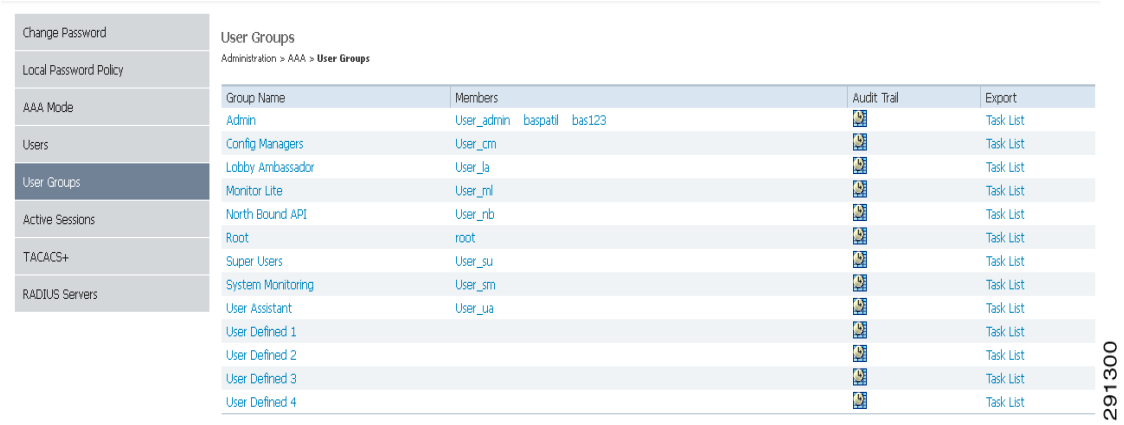
Adding NCS User Groups into ACS for TACACS+

To add NCS User Groups into an ACS Server for use with TACACS+ servers, follow these steps:

Step 1 Log in to the NCS.

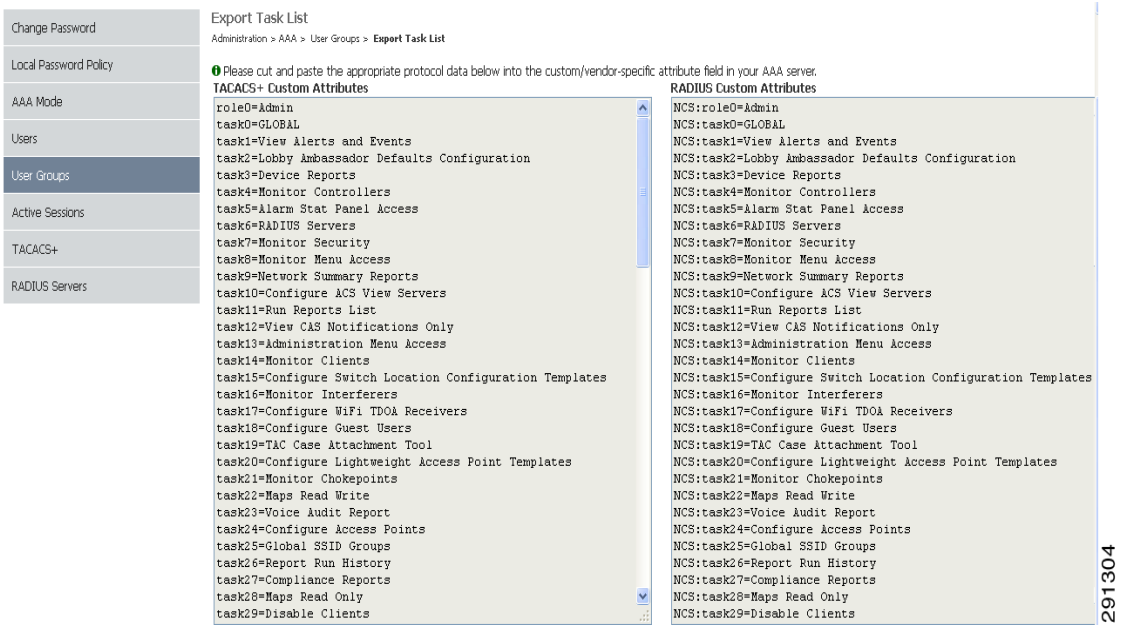
Step 2 Choose **Administration > AAA > User Groups**. The User Groups page appears (see Figure 15-33).

Figure 15-33 User Groups Page



Step 3 Click the Task List link of the user group that you want to add to ACS. The Export Task List page appears (see Figure 15-34).

Figure 15-34 Export Task List Page

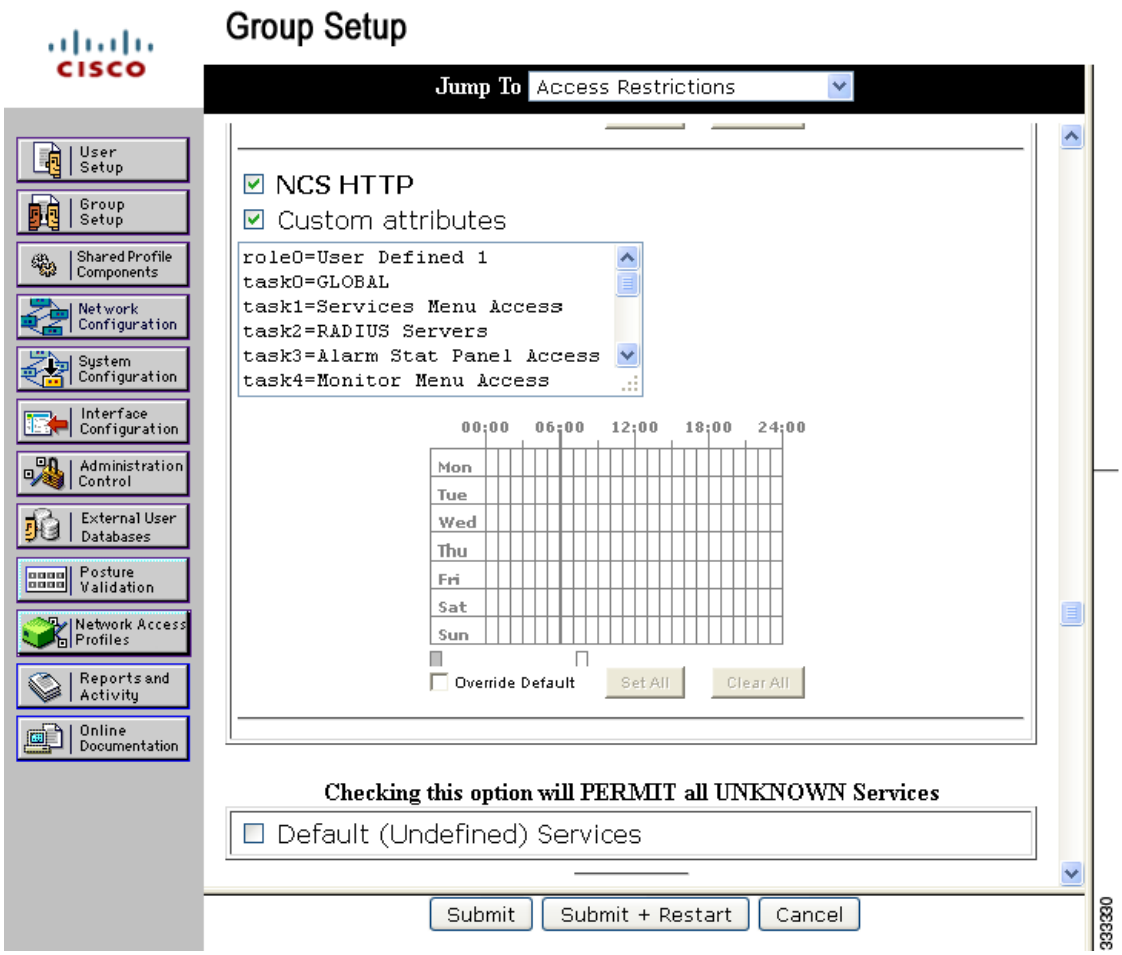


Step 4 Highlight the text inside of the TACACS+ Custom Attributes, go to the menu of your browser, and choose **Edit > Copy**.

Step 5 Log in to ACS.

Step 6 Go to Group Setup. The Group Setup page appears (see Figure 15-35).

Figure 15-35 Group Setup Page on ACS Server



Step 7 Choose which group to use, and click **Edit Settings**. NCS HTTP appears in the TACACS+ setting.

Step 8 Use Edit > Paste in your browser to place the TACACS+ custom attributes from the NCS into this text box.

Note When you upgrade the NCS, any permissions on the TACACS+ or RADIUS server must be readded.

Step 9 Select the check boxes to enable these attributes.

Step 10 Click **Submit + Restart**.

You can now associate ACS users with this ACS group.

Note To enable TACACS+ in the NCS, see the "Configuring TACACS+ Servers" section on page 15-95. For information on configuring ACS view server credentials, see the "Configuring ACS View Server Credentials" section on page 8-247. For information on adding the NCS virtual domains into ACS for TACACS+, see the "Virtual Domain RADIUS and TACACS+ Attributes" section on page 15-49.

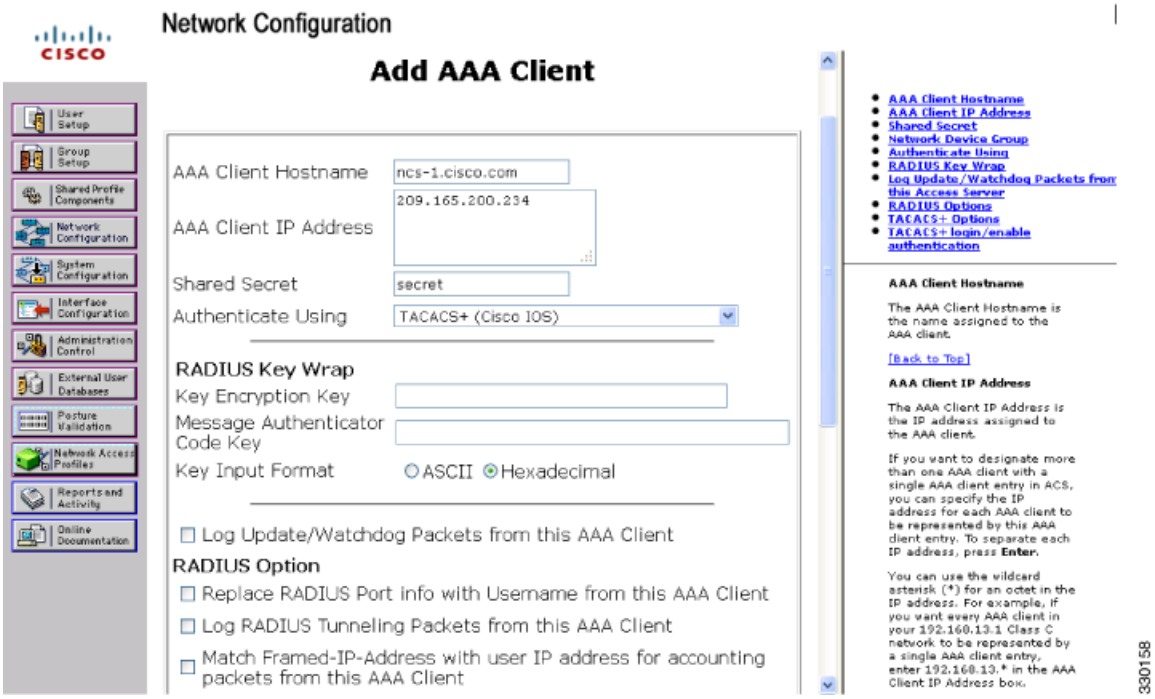
Note From NCS Release 1.0 and later, you are required to add a virtual domain in ACS when exporting the task list to ACS. This might be the default ROOT-DOMAIN virtual domain. For more information on virtual domains, see the "Configuring a Virtual Domain" section on page 15-41.

Adding the NCS to an ACS Server for Use with RADIUS

To add the NCS to an ACS server for use with RADIUS servers, follow these steps. If you have a non-Cisco ACS server, see the "Adding the NCS to a Non-Cisco ACS Server for Use with RADIUS" section on page 15-112.

Step 1 Go to Network Configuration on the ACS server (see Figure 15-36).

Figure 15-36 Network Configuration Page on ACS Server



Step 2 Click **Add Entry**.

Step 3 In the AAA Client Hostname text box, enter the NCS hostname.

Step 4 In the AAA Client IP Address text box, enter the NCS IP address.

Note Ensure the interface that you use for ACS is the same you specified in the NCS and it is reachable.

Step 5 In the Shared Secret text box, enter the shared secret that you want to configure on both the NCS and ACS servers.

Step 6 Choose **RADIUS (Cisco IOS/PIX 6.0)** from the Authenticate Using drop-down list.

Step 7 Click **Submit + Apply**.

You can now associate ACS users with this ACS group.

Note To enable RADIUS in the NCS, see the "Configuring RADIUS Servers" section on page 15-98. For information on configuring ACS view server credentials, see the "Configuring ACS View Server Credentials" section on page 8-247.

Note From NCS Release 1.0 and later, you are required to add a virtual domain in ACS when exporting the task list to ACS. This might be the default ROOT-DOMAIN virtual domain. For more information on virtual domains, see the "Configuring a Virtual Domain" section on page 15-41.

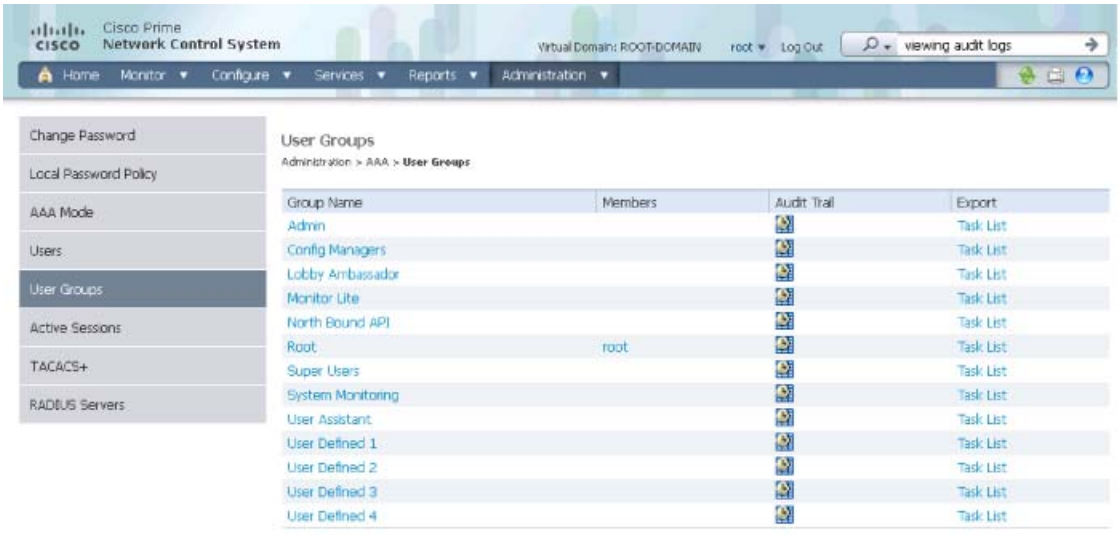
Adding NCS User Groups into ACS for RADIUS

To add NCS user groups into an ACS Server for use with RADIUS servers, follow these steps:

Step 1 Log in to NCS.

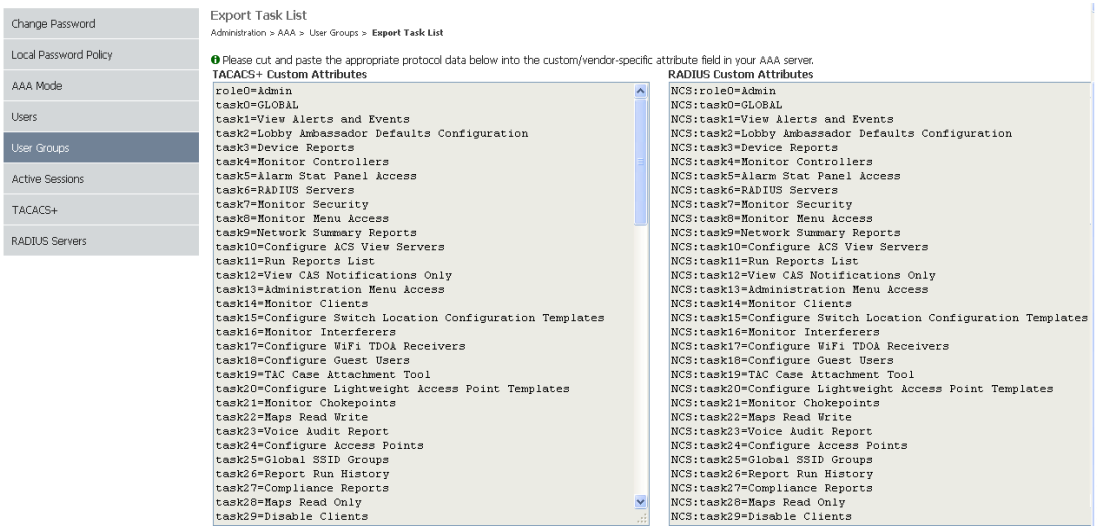
Step 2 Choose **Administration > AAA > User Groups**. The All Groups page appears (see Figure 15-37).

Figure 15-37 User Groups Page



Step 3 Click the Task List link of the user group that you want to add to ACS. The Export Task List page appears (see Figure 15-38).

Figure 15-38 Export Task List Page



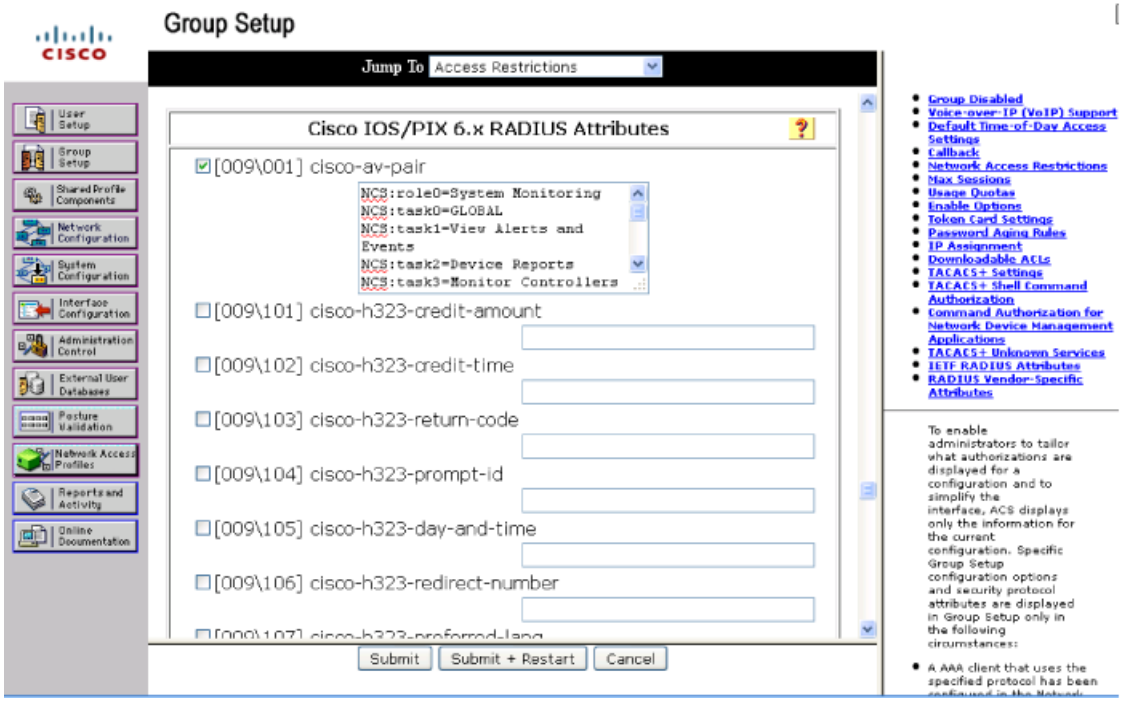
Step 4 Highlight the text inside of the RADIUS Custom Attributes, go to the menu of your browser, and choose **Edit > Copy**.

Note When you upgrade the NCS, any permissions on the TACACS+ or RADIUS server must be readded.

Step 5 Log in to ACS.

Step 6 Go to Group Setup. The Group Setup page appears (see Figure 15-39).

Figure 15-39 Group Setup Page on ACS Server



Step 7 Choose which group to use, and click **Edit Settings**. Find [009\001]cisco-av-pair under Cisco IOS/PIX 6.x RADIUS Attributes.

Step 8 Use Edit > Paste in your browser to place the RADIUS custom attributes from the NCS into this text box.

Note When you upgrade the NCS, any permissions on the TACACS+ or RADIUS server must be readded.

Step 9 Select the check boxes to enable these attributes.

Step 10 Click **Submit + Restart**.

You can now associate ACS users with this ACS group.

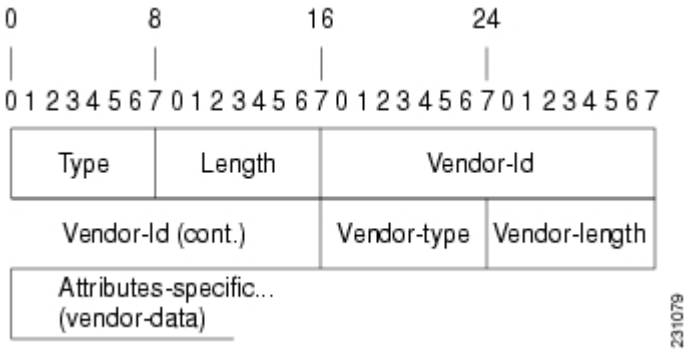
Note To enable RADIUS in the NCS, see the "Configuring RADIUS Servers" section on page 15-98. For information on configuring ACS view server credentials, see the "Configuring ACS View Server Credentials" section on page 8-247. For information on adding NCS virtual domains into ACS for TACACS+, see the "Virtual Domain RADIUS and TACACS+ Attributes" section on page 15-49.

Note From NCS Release 1.0 and later, you are required to add a virtual domain in ACS when exporting the task list to ACS. This might be the default ROOT-DOMAIN virtual domain. For more information on virtual domains, see the "Configuring a Virtual Domain" section on page 15-41.

Adding the NCS to a Non-Cisco ACS Server for Use with RADIUS

When you use a RADIUS server to log in to the NCS, the AAA server sends back an access=accept message with a user group and a list of available tasks, after the username and password were verified. The access=accept message comes back as a fragmented packet because of the large number of tasks in some user groups. You can look in the following file to see the tasks associated with a given user group: C:\Program Files\NCS\webnms\webacs\WEB-INF\security\usergroup-map.xml. The tasks are passed back as a vendor specific attribute (VSA), and the NCS requires authorization information using the VSA (IETF RADIUS attribute number 26). The VSA contains the NCS RADIUS task list information (see Figure 15-40).

Figure 15-40 Extracting Task List



The content of the VSA is as follows:

- Type = 26 (IETF VSA number)
- Vendor Id = 9 (Cisco vendor ID)
- Vendor Type = 1 (Custom attributes)
- Vendor Data = The NCS task information (for example NCS: task0 = Users and Group)

Each line from the NCS RADIUS task list should be sent in its own RADIUS VSA.

In the data portion of the access=access packet, the truncated output sometimes shows only one role sent back for an Admin user group login. The tasks associated with the role start with task0 and increment with task1, task2, and so on. Table 15-8 defines what these attributes in the access=access packet example signify.

```
0000 06 6d 0e 59 07 3d 6a 24 02 47 07 35 d2 12 a4 eb .m.Y.=j$G.5...
0010 a2 5a fa 84 38 20 e4 e2 3a 3a bc e5 1a 20 00 00 .Z..8..:::..
0020 00 09 01 1a 57 69 72 65 6c 65 73 73 2d 57 43 53 ....NCS
0030 3a 72 6f 6c 65 30 3d 41 64 6d 69 6e 1a 2b 00 00 :role0=Admin.+...
0040 00 09 01 25 57 69 72 65 6c 65 73 73 2d 57 43 53 ...%NCS
0050 3a 74 61 73 6b 30 3d 55 73 65 72 73 20 61 6e 64 :task0=Users and
0060 20 47 72 6f 75 70 73 1a 27 00 00 00 09 01 21 57 Groups.”....!W
0070 69 72 65 6c 65 73 73 2d 57 43 53 3a 74 61 73 6b NCS:task
0080 31 3d 41 75 64 69 74 20 54 72 61 69 6c 73 xx xx 1=Audit Trails.*
```

Table 15-8 Access=Access Packet Example

Attribute	Description
1a (26 in decimal)	Vendor attribute
2b (43 bytes in decimal)	Length as the total number of bytes to skip and still reach the next TLV (for task0, Users and Groups)
4-byte field	Vendor Cisco 09
01	Cisco AV pair - a TLV for the NCS to read
25 (37 bytes in decimal)	Length
hex text string	NCS:task0=Users and Groups
	The next TLV until the data portion is completely processed.
255.255.255.255	TLV: RADIUS type 8 (framed IP address)
Type 35 (0x19)	A class, which is a string
Type 80 (0x50)	Message authenticator

To troubleshoot, perform the following steps:

- Verify if the RADIUS packet is an access accept.
- Verify the task names for the user group in the access accept.
- Look at the different length fields in the RADIUS packet.

Configuring ACS 5.x

This section provides instructions for configuring ACS 5.x to work with the NCS.

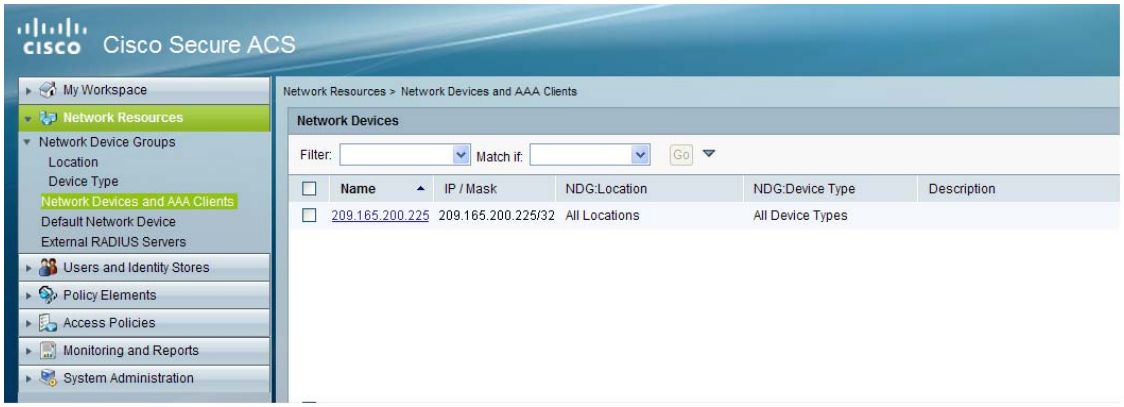
This section contains the following topics:

Creating Network Devices and AAA Clients

To create Network Devices and AAA Clients, follow these steps:

Step 1 Choose **Network Resources > Network Devices and AAA Clients**.

Figure 15-41 Network Devices Page



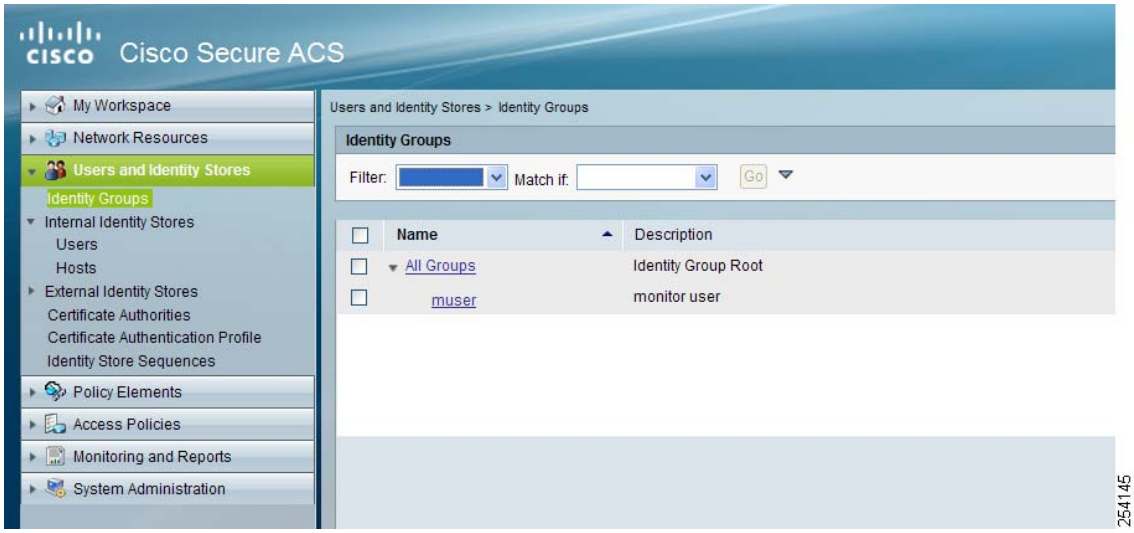
Step 2 Enter an IP address.

Adding Groups

To add groups, follow these steps:

Step 1 Choose **Users and Identity Stores > Identity Groups**.

Figure 15-42 Identify Groups Page



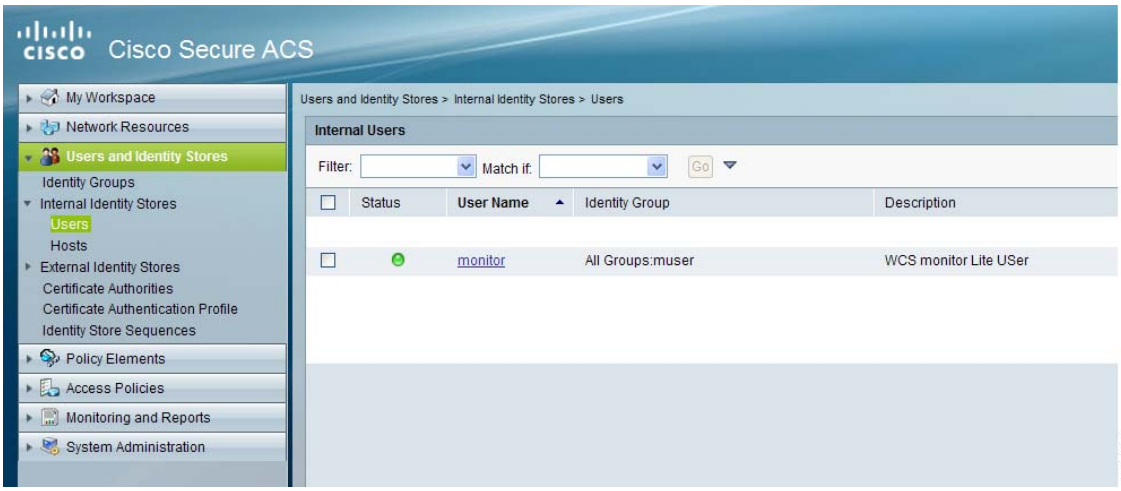
Step 2 Create a Group.

Adding Users

To add users, follow these steps:

Step 1 Choose **Users and Identity Stores > Internal Identity Stores > Users**.

Figure 15-43 Internal Users Page



Step 2 Add a user, and then map to group to that user.

Creating Policy Elements or Authorization Profiles

This section contains the following topics:

- Creating Policy Elements or Authorization Profiles for RADIUS, page 15-115
- Creating Policy Elements or Authorization Profiles For TACACS, page 15-116

Creating Policy Elements or Authorization Profiles for RADIUS

To create policy elements or authorization profiles for RADIUS, perform the following steps:

Step 1 Choose **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**.

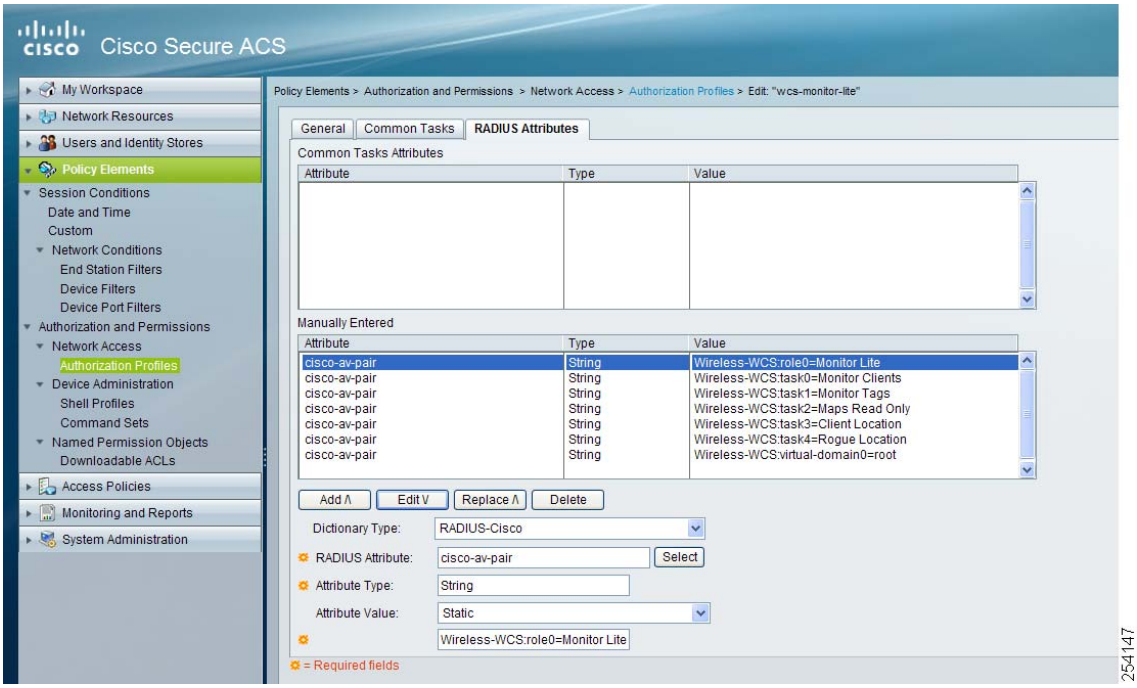
Step 2 Click **Create**.

Step 3 Enter a name and description.

Step 4 Click the **RADIUS Attributes** tab.

Step 5 Add RADIUS attributes one by one (see Figure 15-44).

Figure 15-44 Authorization Profiles Page



Step 6 Click **Submit**.

Creating Policy Elements or Authorization Profiles For TACACS

To create policy elements or authorization profiles for TACACS, perform the following steps:

Step 1 Choose **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**.

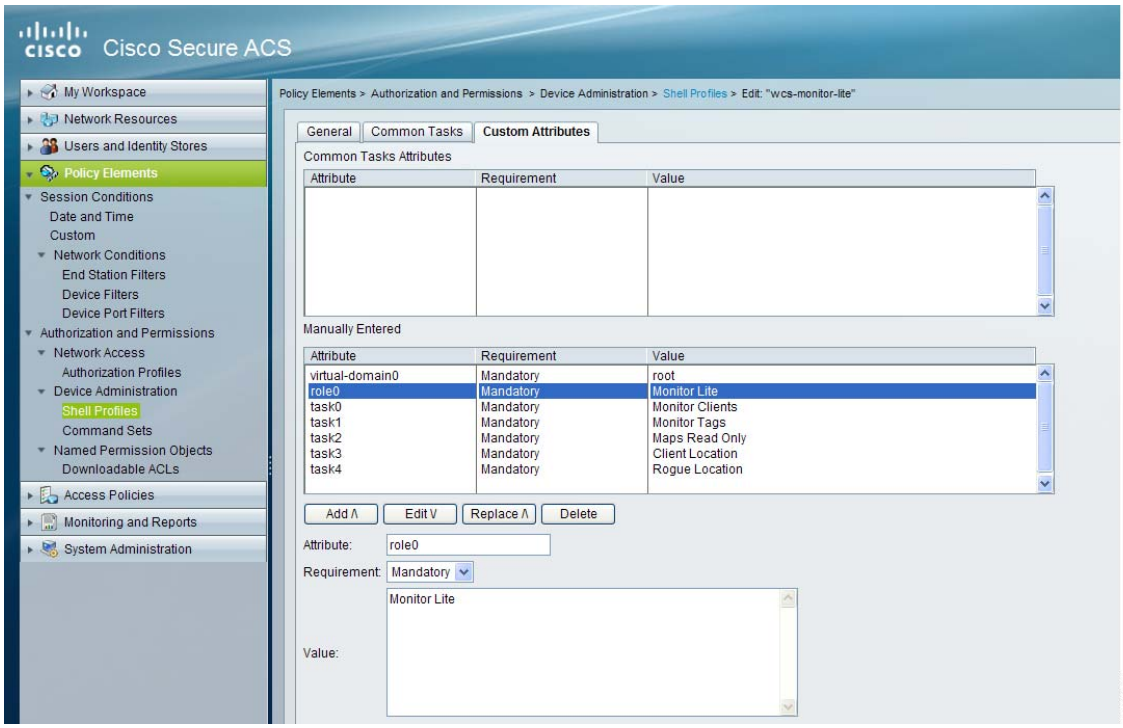
Step 2 Click **Create**.

Step 3 Enter a name and description.

Step 4 Click the **Custom Attributes** tab.

Step 5 Add the TACACS ttributes one by one (see Figure 15-45).

Figure 15-45 Shell Profiles Page



Step 6 Click **Submit**.

Creating Authorization Rules

This section provides instructions for configuring authorization for RADIUS and TACACS.

This section contains the following topics:

- "Creating Service Selection Rules for RADIUS" section on page 15-117
- "Creating Service Selection Rules for TACACS" section on page 15-118

Creating Service Selection Rules for RADIUS

To create service selection rules for RADIUS, perform the following steps:

Step 1 Choose **Access Policies > Access Services > Service Selection Rules**.

Step 2 Click **Create**.

Step 3 Select the protocol as Radius and choose **Default Network Access** from the Service drop-down list. (see Figure 15-46).

Figure 15-46 Service Selection Page

Step 4 Click **OK**.

Creating Service Selection Rules for TACACS

To create service selection rules for TACACS, follow these steps:

Step 1 Choose **Access Policies > Access Services > Service Selection Rules**.

Step 2 Click **Create**.

Step 3 Select the protocol as TACACS and choose **Default Device Admin** from the Service drop-down list. (see Figure 15-47).

Figure 15-47 Service Selection Page

Step 4 Click **OK**.

Configuring Access Services

This section provides instructions for configuring access services for RADIUS and TACACS.

This section contains the following topics:

Configuring Access Services for RADIUS

To configure access services for RADIUS, perform the following steps:

Step 1 Log in to the ACS 5.x server and choose **Access Policies > Access Services > Default Network Access**.

Step 2 On the General tab, select the policy structure you want to use. By default, all the three policy structures are selected.

Step 3 From the Allowed Protocols, select the protocols you want to use.

Note You can retain the defaults for identity and group mapping.

Step 4 To create an authorization rule for RADIUS, choose **Access Policies > Access Services > Default Network Access > Authorization** (see Figure 15-48).

Step 5 Click **Create**.

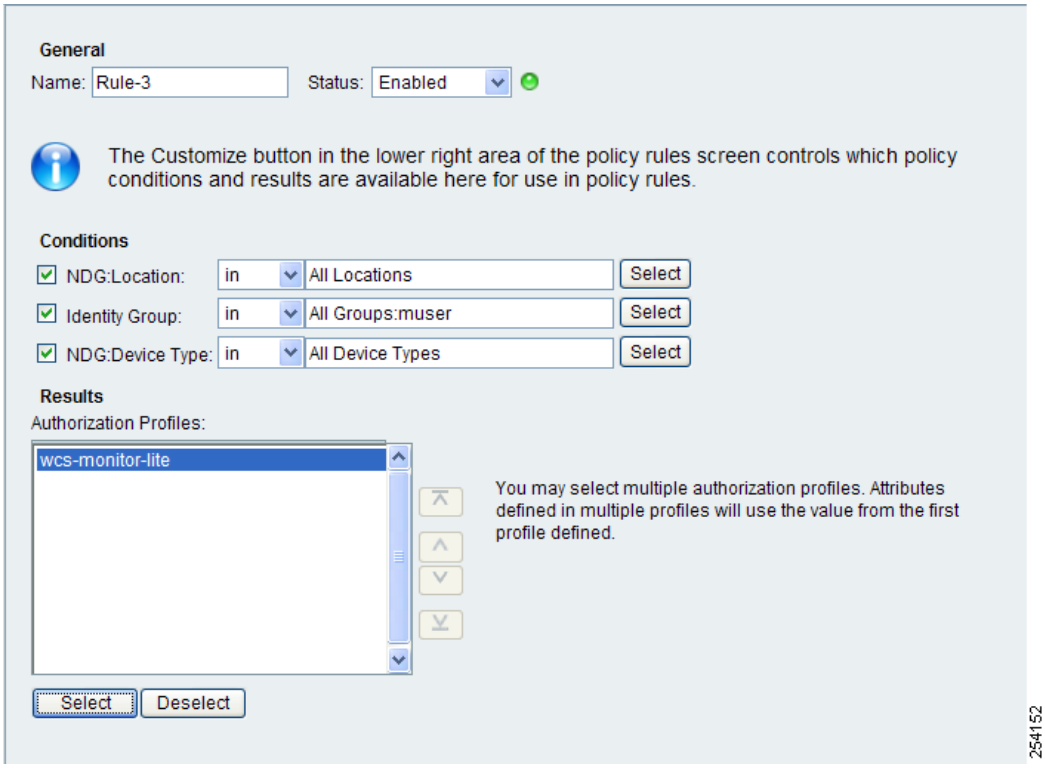
Step 6 In Location, select **All Locations** or you can create a rule based on the location.

Step 7 In Group, select the group that you created earlier.

Step 8 In Device Type, select **All Device Types** or you can create a rule based on the Device Type.

Step 9 In Authorization Profile, select the authorization profile created for RADIUS.

Figure 15-48 Authorization Page



Step 10 Click **OK**.

Step 11 Click **Save**.

Configuring Access Services for TACACS

To configure access services for TACACS, follow these steps:

Step 1 Choose **Access Policies > Access Services > Default Device Admin**.

Step 2 On the General tab, select the policy structure you want to use. By default, all the three are selected. Similarly, in Allowed Protocols, select the protocols you want to use.

Note You can retain the defaults for identity and group mapping.

Step 3 To create an authorization rule for TACACS, choose **Access Policies > Access Services > Default Device Admin > Authorization**. (see Figure 15-49).

Step 4 Click **Create**.

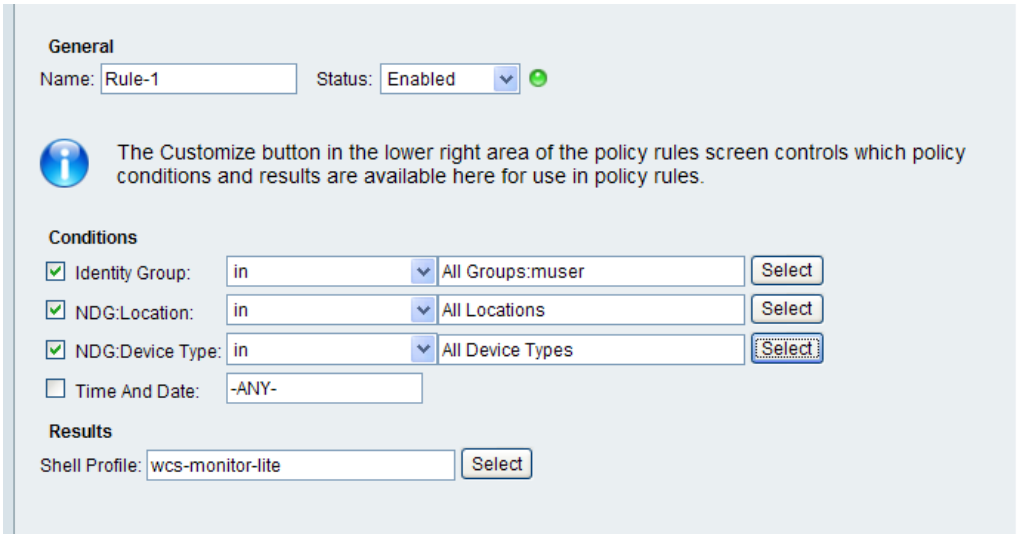
Step 5 In Location, select All Locations or you can create a rule based on the location.

Step 6 In Group, select the group that you created earlier.

Step 7 In Device Type, select All Device Types or you can create a rule based on the Device Type.

Step 8 In Shell Profile, select the shell profile created for TACACS.

Figure 15-49 Authorization Page



Step 9 Click **OK**.

Step 10 Click **Save**.

Establishing Logging Options

Choose **Administration > Logging** to access the Administer Logging Options page. The logging for controller syslog information can be done in the Controller > Management > Syslog page. This section describes the log settings that can be configured and contains the following topics:

- General Logging Options, page 15-121
- SNMP Logging Options, page 15-123
- Syslog Options, page 15-124

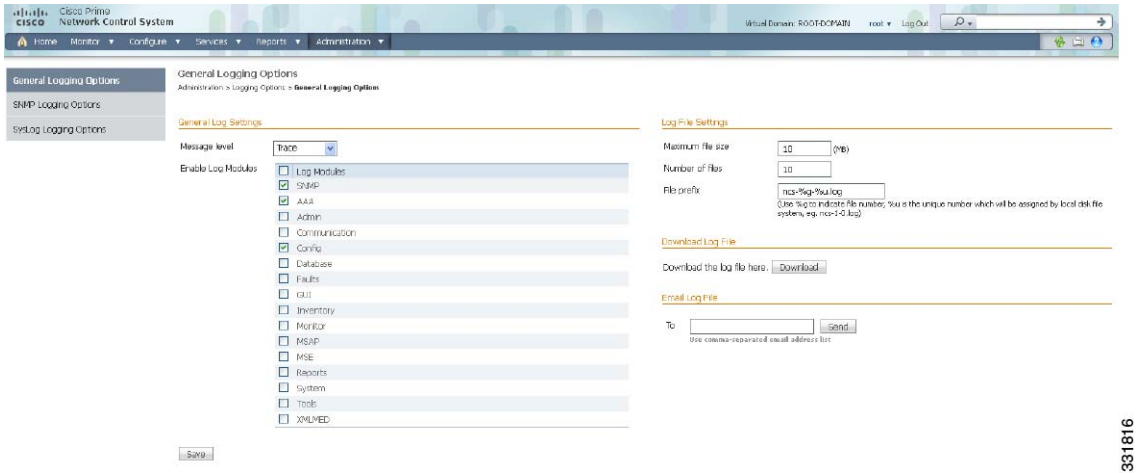
General Logging Options

To enable e-mail logging, follow these steps. The settings you establish are stored and are used by the e-mail server.

Step 1 Choose **Administration > Logging**. The General Logging Options page appears (see Figure 15-50).

Step 2 Choose **General Logging Options** from the left sidebar menu.

Figure 15-50 General Logging Options Page



Step 3 From the Message level drop-down list, choose **Trace**, **Information**, or **Error**.

Step 4 Select the check boxes within the Enable Log Module group box to enable various administration modules:

- Message Level—Select the minimum level of the messages that are logged including **Error**, **Information**, or **Trace**.
- Enable Log Module—You can enable logging for the following administration modules:
  - Log Modules—Select this check box to select all the modules.
  - SNMP—Captures logs for all SNMP communication between the NCS and controllers.
  - AAA—Captures AAA related logs for the NCS.
  - Admin—Contains Administration based logs, where all the configuration changes performed using the administration console is logged.
  - Communication—Contains logs related to the protocols used in communication.
  - Config—Used to log controller configurations that you make from the NCS.

    Note To get complete controller configuration logs, also enable the General log module.

    Note To get the configuration values that the NCS sends in logs to controllers, enable Trace Display Values (Administration > Settings > SNMP Settings > Trace Display Value).

  - Database—Contains logs to debug important database-related operations in the NCS.

    Note Some functions should be used only for short periods of time during debugging so that the performance is not degraded. For example, trace mode and SNMP meditation should be enabled only during debugging because a lot of log information is generated.

  - Faults—Used by the event and alert subsystem.
  - GUI—Contains generic UI validation logs.

- Inventory—Captures all Inventory-related logs.
- Monitor—Used for Alarms, Spectrum Intelligence, CCXV5, Clients/Tags, Client Radio Measurements, SSO, and Mesh.
- MSE—Used for MSE-related operations such as adding or deleting an MSE and changing parameters on the MSE. It also enables logging for MSE synchronization including NW designs and controllers.
- Reports—Used to log messages related to creating, saving, scheduling, and running reports. This module also contains a list of scheduled and saved reports.
- System—Captures all System-related logs.
- Tools—Contains logs related to different plug-in tools.
- XMLMED—Used to enable trace for the communication between the MSE and NCS.

Step 5 In the Log File Settings portion, enter the following settings. These settings become effective after restarting NCS.

- Max. file size—Maximum number of MBs allowed per log file.
- Number of files—Maximum number of log files allowed.
- File prefix—Log file prefix, which can include the characters "%g" to sequentially number of files.

Step 6 Click **Download** to download the log file to your local machine.

Note The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the .zip file is an html file that documents the log files.

Step 7 Enter the E-mail ID or E-mail IDs separated by commas to send the log file.

Note To send the log file in a mail you must have E-mail Server configured.

Step 8 Click **Submit**.

SNMP Logging Options

To enable SNMP Tracing, follow these steps. The settings you establish are stored and are used by the SNMP server.

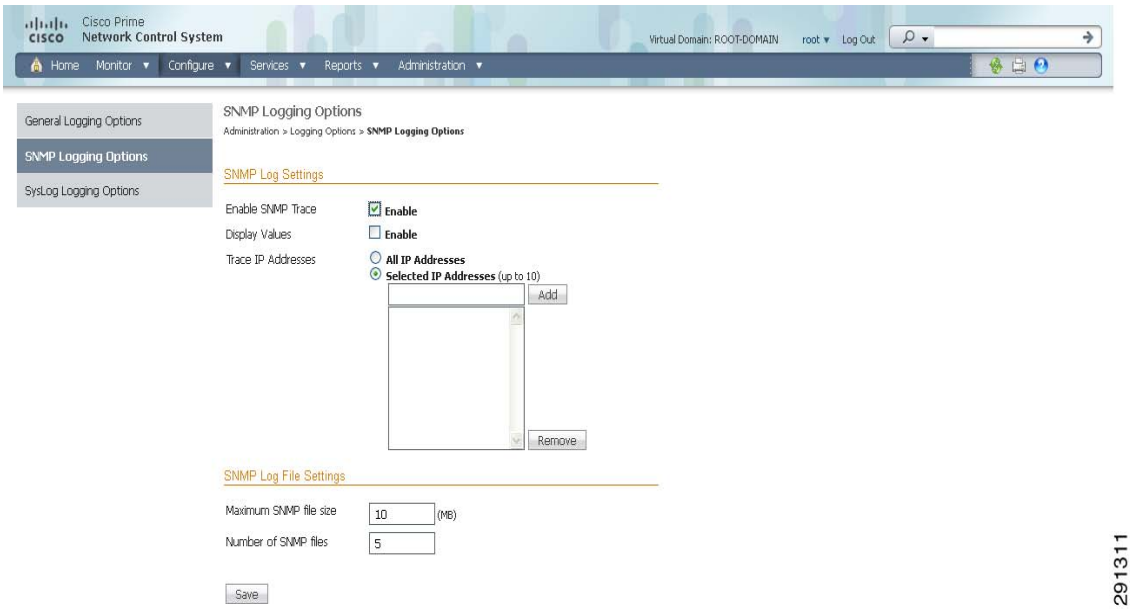
Note SNMP server is nothing but the NCS server which uses these settings for SNMP logging.

Note When you upgrade from WCS Release 7.x to NCS Release 1.1, the settings under Administration > Logging Options > SNMP Logging Options are not retained.

Step 1 Choose A**dministration > Logging**. The Logging Options page appears (see Figure 15-51).

Step 2 Choose the **SNMP Logging Options** from the left sidebar menu.

Figure 15-51 SNMP Logging Options Page



Step 3 Select the **Enable SNMP Trace** check box to enable sending SNMP messages (along with traps) between controller and NCS.

Step 4 Select the **Display Values** check box to see the SNMP Message values.

Step 5 Configure the IP address or IP addresses to trace the SNMP traps. You can add up to a maximum of 10 IP addresses in the text box.

Step 6 You can configure the maximum SNMP file size and the number of SNMP files.

Syslog Options

The Syslog protocol is simply designed to transport event messages from the generating device to the collector. Various devices generate syslog messages for system information and alerts.

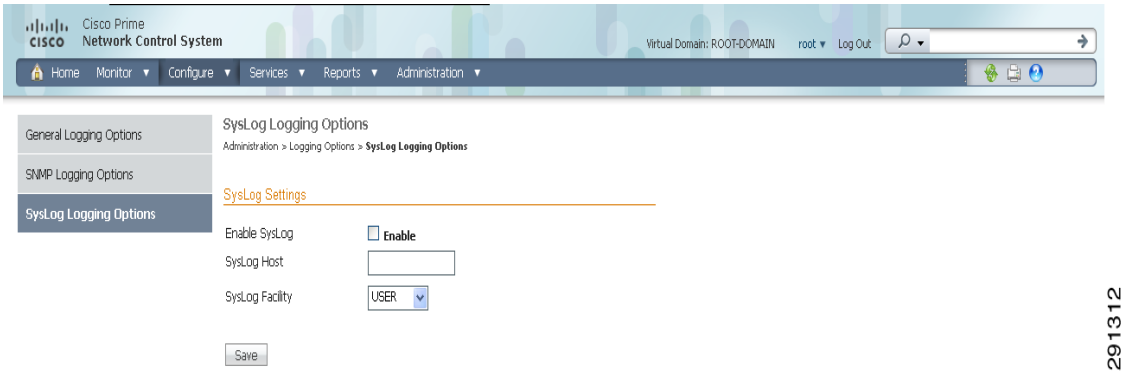
Note When you upgrade from WCS Release 7.x to NCS Release 1.1, the settings under Administration > Logging Options > SysLog Logging Options are not retained.

To configure Syslog for the NCS, follow these steps:

Step 1 Choose A**dministration > Logging**. The Logging Options page appears (see Figure 15-50).

Step 2 Choose the **Syslog Options** from the left sidebar menu.

Figure 15-52 Syslog Options Page



Step 3 Select the **Enable Syslog** check box to enable collecting and processing system logs.

Step 4 Configure the Syslog Server IP address of the interface from which the message is to be transmitted.

Step 5 Choose the **Syslog Facility**. You can choose any of the eight local use facilities for sending syslog messages. The local use facilities are not reserved and are available for general use.

Using Logging Options to Enhance Troubleshooting

The logging page allows you to customize the amount of data the NCS collects to debug an issue. For easily reproduced issues, follow these steps prior to contacting TAC. These steps might create a smoother troubleshooting session:

Step 1 Choose **Administration > Logging**.

Step 2 From the Message Level drop-down list, choose **Trace**.

Step 3 Select each check box to enable all log modules.

Step 4 Reproduce the current problem.

Step 5 Return to the Logging Options page.

Step 6 Click **Download** from the Download Log File section.

Note The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the .zip file is an html file that documents the log files.

Step 7 After you have retrieved the logs, choose **Information** from the Message Level drop-down list.

Note Leaving the Message Level at *Trace* can adversely affect performance over a long period of time.

Configuring High Availability

To ensure continued operation in case of failure, the NCS now provides a high availability or failover framework. When an active (primary) NCS fails, a secondary NCS takes over operations (in less than two minutes) for the failed primary NCS and continues to provide service. Upon failover, a peer of the failed primary NCS is activated on the secondary NCS using the local database and files, and the secondary NCS runs a fully functional NCS. While the secondary host is in failover mode, the database and file backups of other primary NCSs continue uninterrupted.

If E-mail Address is specified in the HA configuration, Mail Server must be configured and reachable to succeed in HA configuration.

For more high availability information, see the following sections:

- Guidelines and Limitations for High Availability, page 15-126
- Failover Scenario, page 15-127
- Performing Background Tasks, page 15-1
- High Availability Status, page 15-127
- Configuring High Availability on the Primary NCS, page 15-128
- Deploying High Availability, page 15-130

This section contains the following topics:

Guidelines and Limitations for High Availability

Before initiating failover, you must consider the following prerequisites and limitations:

- You must have the extra hardware identical to the primary NCS to run a standby instance of the NCS.
- The NCS supports High Availability on both the physical and virtual appliance deployment models.
- A reliable high speed wired network must exist between the primary NCS and its backup NCS.
- The primary and secondary NCS must be running the same NCS software release.
- Failover should be considered temporary. The failed primary NCS should be restored to normal as soon as possible, and failback is reinitiated. The longer it takes to restore the failed primary NCS, the longer the other NCSs sharing that secondary NCS must run without failover support.
- The latest controller software must be used.
- The primary and secondary host are not required to share the same subnet. They can be geographically separated.
- If a secondary host fails for any reason, all the primary instances are affected, and they run in stand-alone mode without any failover support.

- The ports over which the primary and secondary NCSs communicate must be open (not blocked with network firewalls, application fireways, gateways, and so on). The tomcat port is configurable during installation, and its default port is 8082. You should reserve solid database ports from 1315 to 1319.
- Any access control lists imposed between the primary and secondary NCS must allow traffic to go between the primary and secondary NCSs.

NCS 1.x Updates for High Availability

- In NCS Release 1.x, a secondary NCS can only support one primary NCS.
- When high availability is enabled for the first time, the sync up of the servers take a considerable amount of time. The time it would take would be in the order of 30 minutes or more depending on the size of the database.

Failover Scenario

When a failure of a primary NCS is automatically detected, the following events take place:

Note One physical secondary NCS can back many primary devices (NCS).

1. The primary NCS is confirmed as non-functioning (hardware crash, network crash, or the like) by the health monitor on the secondary NCS.
2. If automatic failover has been enabled, NCS is started on the secondary as described in Step 3. If automatic failover is disabled, an e-mail is sent to the administrator asking if they want to manually start failover.
3. The secondary NCS instance is started immediately (using the configuration already in place) and uses the corresponding database of the primary. After a successful failover, the client should point to the newly activated NCS (the secondary NCS). The secondary NCS updates all controllers with its own address as the trap destination.

   Note The redirecting of web traffic to the secondary NCS does not occur automatically. You must use your infrastructure tools to properly configure this redirection.

4. The result of the failover operation is indicated as an event in the Health Monitor UI, or a critical alarm is sent to the administrator and to other NCS instances.

High Availability Status

To view high availability details, follow these steps:

Step 1 Choose **Administration > High Availability**.

Step 2 Choose **HA Status** from the left sidebar menu. The following information is displayed:

- Current status

- Time, state, and description of each event

Table 15-9 provides details about the different statuses of High Availability.

Table 15-9 High Availability Statuses

HA Status	Description
Stand Alone	HA is not configured.
Primary Alone	The primary NCS is alone and not synching with the secondary NCS.
HA Initializing	HA is initializing.
Primary Active	HA is synching with the secondary NCS without issue.
Primary Lost Secondary	The primary NCS has lost connectivity with the secondary NCS.
Primary Failover	A failover is being done to the primary NCS.
Primary Failback	A failback to the primary NCS is being done.
Primary Uncertain	The primary NCS is uncertain about the state of the secondary NCS.
Secondary Alone	The secondary NCS is alone and not synching with the primary NCS.
Secondary Syncing	HA is synching with the primary NCS without issue.
Secondary Active	HA has failed over the primary NCS and the application is running on the secondary NCS and is active.
Secondary Lost Primary	The secondary NCS has lost connectivity with the primary NCS.
Secondary Failover	A failover is being done to the secondary NCS.
Secondary Failback	A failback to the secondary NCS is being done.
Secondary Post Failback	A failback is in the post step.
Secondary Uncertain	The secondary NCS is uncertain about the state of the primary NCS.

Configuring High Availability on the Primary NCS

Note When database transaction logs grow to 1/3 of the database partition disk space, set the database to "Standalone" mode to prevent transaction logs from growing. But it requires a complete *netcopy* next time when the database synchronization occurs.

Follow these steps to configure high availability on the primary NCS. You must specify the NCS role (either standalone, primary, or secondary) during installation. See the "Deploying the NCS Virtual Appliance" section on page 2-6 to see the installation steps.

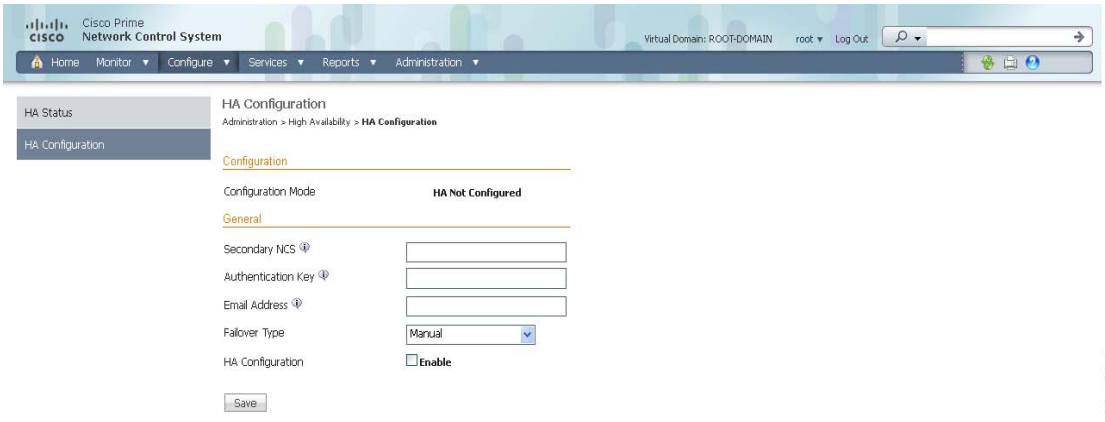
Note

- Before you configure high availability, you must configure a mail server. See the "Configuring the Mail Server" section on page 15-63 for steps on configuring a mail server.
- If you specify an e-mail address in the HA Configuration page then ensure a mail server is configured and reachable.

Step 1 Choose **Administration > High Availability**.

Step 2 Choose **HA Configuration** from the left sidebar menu. The High Availability Configuration page appears (see Figure 15-53).

Figure 15-53 High Availability Configuration Page



The current status of high availability is shown in the upper portion of the page. For information about different statuses of High Availability, see Table 15-9.

Step 3 Enter the IP address or hostname of the secondary NCS.

Step 4 Enter the authentication key specified during the installation of the secondary NCS.

Step 5 The default admin e-mail address that you configured in Administration > Settings > E-mail Server is automatically supplied. You can make any necessary changes. Any changes you make to these e-mail addresses must also be entered in the Secondary SMTP Server section of the Administration > Settings > Mail Server page.

Note You must enter an e-mail address when configuring high availability. The NCS tests the e-mail server configuration, and if the test fails (because the mail server cannot connect), the NCS does not allow the high availability configuration.

Step 6 From the Failover Type drop-down list, choose either manual or automatic. If you choose manual, you can trigger the failover operation with a button in the secondary HealthMonitor graphical user interface or with the URL specified in the e-mail which the administrator receives upon failure of the primary NCS. If you choose automatic, the secondary NCS initiates a failover on its own when a failure is detected on the primary.

Step 7 Click **Save** to retain the configuration and enable high availability, or click **Remove** to disable high availability and its settings.

Note The Remove button is only available if high availability is already configured.

At this point, the secondary is either reachable with the database, and files are synchronized between health monitors, or the secondary is unreachable, and an error is returned because secondary installation did not occur.

From the NCS graphical user interface (Administration > High Availability) after high availability has been enabled, you can perform the following functions:

- Update—Use the Update function to make changes to the Report Repository path (Administration > Settings > Report) or FTP/TFTP root directory (Administration > Settings > Server Settings) and to appropriately synchronize the files.
- Delete—Use the Delete operation to decommission the primary NCS from the secondary NCS.
- Cancel—Use the Cancel operation to cancel any modifications you made to the high availability configuration. You are returned to the High Availability Status page after you choose Cancel.

Deploying High Availability

To deploy high availability on an existing NCS installation, follow these steps:

Step 1 Identify and prepare the hardware to run the secondary NCS.

Step 2 Ensure that network connectivity between the primary and secondary NCS is functioning, and all necessary ports are open.

Step 3 Install the secondary NCS with the same version of the NCS that is installed on the primary. See the "Deploying the NCS Virtual Appliance" section on page 2-6.

Step 4 Start the secondary NCS as a standby server. In this mode, the NCS application does not start. At the same time, the Health Monitor is started on the secondary NCS.

Step 5 On every primary NCS that needs to use this secondary NCS, stop the NCS.

Step 6 On the primary host, install the new version of NCS and perform all necessary upgrade steps.

Step 7 Start the primary NCS (as a primary). The Health Monitor also starts.

Step 8 Configure the high availability parameters described in the "Configuring High Availability on the Primary NCS" section on page 15-128.

Step 9 Click **Activate** to activate high availability on the primary. The NCS primary first copies its database to the secondary NCS and then connects to the secondary. The following files are copied over from the primary to the secondary NCS:

- DB password file
- all auto provisioning startup config files
- all domain maps
- all history reports which are generated by scheduled report tasks

High availability deployment is complete. Use https://<ncsip>:8082 to access the HealthMonitor UI. Within the HealthMonitor UI, use the authentication key to log in.

You can change the authentication key in the NCS using the command prompt. To change the authentication key, change the path to the NCS installation directory then to "bin" and enter **hmadmin - authkey** *key*.

To view the current status of the health monitor, enter the **hmadmin [-options] status** command.

Adding a New Primary NCS

To add a new primary NCS to an existing setup, follow these steps. This new primary NCS uses the existing secondary as the failover server.

Step 1 Ensure that network connectivity between the new primary and secondary is functioning and that all necessary ports are open.

Step 2 Make sure that the same NCS release that is loaded on the other primary NCS and secondary NCS is loaded on the new primary NCS.

Step 3 Install the correct version of NCS on the primary NCS.

Step 4 Upgrade the primary NCS. The Health Monitor also starts.

Step 5 Follow the steps in the "Configuring High Availability" section on page 15-126.

Step 6 After the primary NCS connects to the secondary, the Health Monitor on the primary connects to the secondary Health Monitor. They mutually acknowledge each other and start the monitoring.

High availability deployment is now complete.

Removing a Primary NCS

When a primary NCS instance is removed from a group, you must disable the peer database instance on the secondary NCS and remove the Health Monitor for that primary. (To remove the primary NCS from high availability, use the Remove button on the High Availability configuration page.) The secondary NCS disables the database instance and removes the uninstalled primary NCS from its Health Monitor.

Managing Licenses

This section contains the following topics:

License Center

The License Center allows you to manage NCS, wireless LAN controllers, and MSE licenses. The License Center is available from the NCS Administration menu. To view the License Center page, choose **Administration > License Center** (see Figure 15-54).

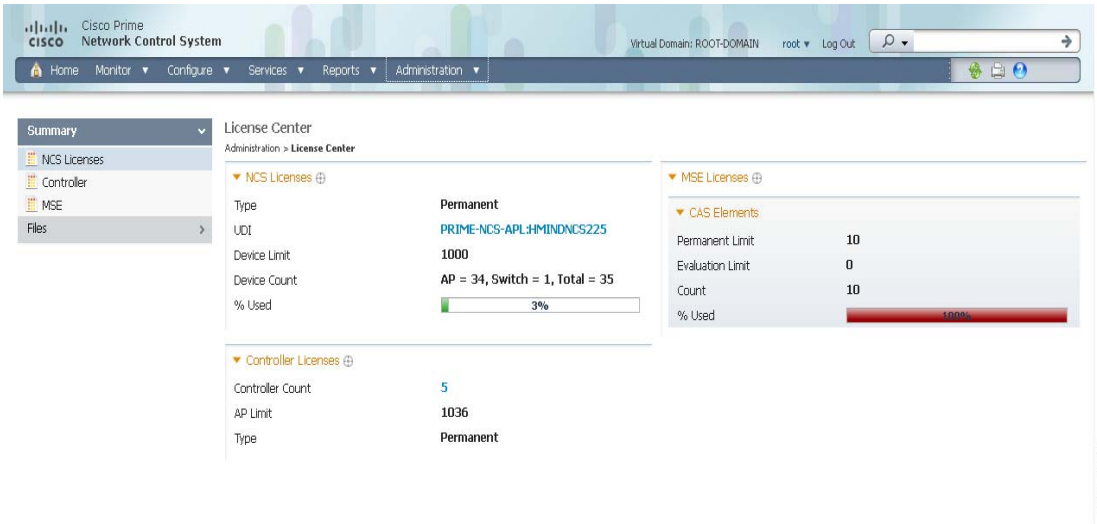
Note Although NCS and MSE licenses can be fully managed from the License Center, WLC licenses can only be viewed. You must use WLC or CLM to manage WLC licenses.

Tip To learn more about the NCS License Center, go to Cisco.com to watch a multimedia presentation. Here you can also find the learning modules for a variety of NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

This section contains the following topics:

For more information about NCS licenses, see the "NCS Licenses" section on page 1-3.

Figure 15-54 License Center



NCS License Information

The NCS Licenses portion of the License Center page displays the following:

- Feature—The type of license. It can be NCS or DEMO.
- Device Limit—The total number of licensed access points and switches.
- Device Count—The current number of access points and switches using licenses.

Note AP count includes both associated and unassociated access points. When you are near the AP limit, you can delete any unassociated access points to increase available license capacity. For a demo license, you can click the "If you do not have a Product Authorization Key (PAK), please click here for available licenses" link and choose **Wireless Control System Trial License**.

Note Autonomous access points are not counted towards the total device count for your license.

- % Used—The percentage of access points and switches licensed across the NCS. If the percentage drops to 75%, the value appears in red. At this level, a message also appears indicating that both associated and unassociated access points are part of the AP count.
- Type—Permanent if all licenses are permanent. If any licenses are evaluations (or demos), it shows the number of days remaining on the license that has the fewest number of days until expiration.

Note To obtain a new license for the NCS, go to the Product License Registration link

(https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet)

and provide your Product Authorization Key (PAK) and hostname.

Note If you choose **Summary > NCS** from the left sidebar menu, only the NCS license information is displayed.

See the *Cisco Wireless Control System Licensing and Ordering Guide* at this URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd804b4646.html#wp9000156.

It covers selecting the correct SKU, ordering the SKU, installing the software, registering the PAK certificate, and installing the license file on the server.

See the "NCS Licenses" section on page B-1 for more information on licensing enforcement, PAK certificates, license types, and installing and managing NCS licenses.

WLC Controller License Information

The Controller Licensing portion of the License Center page provides the following information for both WPLUS and Base licenses:

- Controller Count—The current number of licensed controllers.

Note Only 5500 series controllers are included in the count. The NCS provides only an inventory view and issues warnings if a license is expiring.

Note Clicking the number in this column is the same as choosing **Summary > Controller** from the left sidebar menu, except that it is sorted by the feature you select. This page provides a summary of active controllers.

- AP Limit—The total number of licensed access points.
- Type—The four different types of licenses are as follows:

Note For any controllers with a type other than Permanent, the least number of days left to expiration is shown.

- Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by the licensing portal of Cisco and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
- Evaluation—Licenses are non-node-locked and are valid only for a limited period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license that has the fewest number of days until expiration is shown.
- Extension—Licenses are node-locked and metered. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.
- Grace Period—Licenses are node-locked and metered. These licenses are issued by the licensing portal of Cisco as part of the permission ticket to rehost a license. They are installed on the device as part of the rehost operation, and you must accept a EULA as part of the rehost operation.

If you need to revoke a license from one controller and install it on another, it is called *rehosting*. You might want to rehost a license to change the purpose of a controller. See Chapter 3, "Performing Maintenance Operations," of the *Cisco Wireless LAN Controller Configuration Guide* for information on rehosting a license.

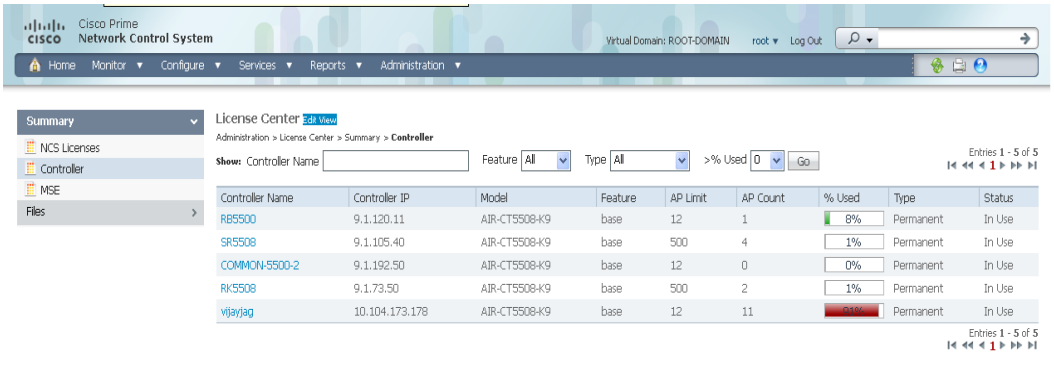
Note The licensing status is updated periodically. To initiate an immediate update, choose **Administration > Background Tasks** and run the Controller License Status task.

If your network contains various Cisco licensed devices, you might want to consider using the Cisco License Manager (CLM) to manage all of the licenses using a single application. CLM is a secure client/server application that manages Cisco software licenses network wide. You can download the CLM software and access user documentation at this URL: http://www.cisco.com/go/clm. You can either register a PAK certificate with CLM or with the licensing portal found at the following URL: https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet.

WLC Controller License Summary

If you want to see more details about controller licensing, from the left sidebar menu, choose the **Summary > Controller**. The License Center page appears (see Figure 15-55). All currently active licenses on the controller are summarized.

Figure 15-55 License Center (Edit View) Page



All licensed controllers and their information in the bulleted list below are displayed. If you want to change how the controller results are displayed, click **Edit View**. In the Edit View page, highlight License Status, and click **Hide** to remove the column from the display.

Above the Controller Summary list is a series of filters that allow you to filter the list by Controller Name, Feature, Type, or Greater Than Percent Used. For example, if you enter 50, the list shows any WLCs that have more than 50% of its licenses used.

Note You can also use the **Advanced Search** link to sort the list of controllers.

- Controller Name—Provides a link to the Files > Controller Files page.
- Controller IP—The IP address of the controller.
- Model—The controller model type.
- Feature—The type of license, either Base or WPLUS. The Base license supports the standard software set, and the WPLUS license supports the premium Wireless Plus (WPLUS) software set. The WPLUS software set provides the standard feature set as well as added functionality for OfficeExtend access points, CAPWAP data encryptions, and enterprise wireless mesh.
- AP Limit—The maximum capacity of access points allowed to join this controller.
- AP Count—The current number of access points using licenses.
- % Used—The percentage of licensed access points that are being used. If the percentage is greater than 75%, the bar appears red to indicate that the limit is being approached.
- Type—The three different types of licenses are as follows:

  Note For any controllers with a type other than Permanent, the least number of days left to expiration is shown.

  – Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.

  - Evaluation—Licenses are non-node-locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license which has the fewest number of days until expiration is shown.
  - Extension—Licenses are node-locked and metered. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.

Note If a license shows as expired, the controller does not stop functioning. Only upon a reboot, the controller with the expired license become inactive.

- Status—In Use, Not in Use, Inactive, or EULA Not Accepted.
  - Inactive—The license level is being used, but this license is not being used.
  - Not In Use—The license level is not being used and this license is not currently recognized.
  - Expired In Use—The license is being used, but is expired and will not be used upon next reboot.
  - Expired Not In Use—The license has expired and can no longer be used.
  - Count Consumed—The ap-count license is In Use.

Mobility Services Engine (MSE) License Information

There are three types of licenses:

- Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
- Evaluation—Licenses are non-node-locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license which has the fewest number of days until expiration is shown.
- Extension—Licenses are node-locked and metered. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.

The MSE Licenses portion of the License Center page provides information for each service. See (Table 15-10).

Table 15-10 MSE License Information

Field	Description
CAS Elements	
Permanent Limit	The total number of CAS elements with permanent licenses.
Evaluation Limit	The total number of CAS elements with evaluation licenses.

Table 15-10 MSE License Information (continued)

Field	Description
CAS Elements	
Count	The number of CAS elements currently licensed across MSEs.
% Used	The percentage of CAS elements licensed across MSEs.
wIPS Monitor Mode APs	
Permanent Limit	The total number of wIPS Monitor Mode APs with permanent licenses.
Evaluation Limit	The total number of wIPS Monitor Mode APs with evaluation licenses.
Count	The number of wIPS Monitor Mode APs currently licensed across MSEs.
% Used	The percentage of wIPS Monitor Mode APs licensed across MSEs.
Under wIPS Monitor Mode Aps or wIPS Local Mode Aps, an active link takes you to a list of licensed access points. You cannot access a list of licensed clients and tags.	
wIPS Local Mode APs	
Permanent Limit	The total number of wIPS Local Mode APs with permanent licenses.
Evaluation Limit	The total number of wIPS Local Mode APs with evaluation licenses.
Count	The number of wIPS Local Mode APs currently licensed across MSEs.
% Used	The percentage of wIPS Local Mode APs licensed across MSEs.
Under wIPS Monitor Mode APs or wIPS Local Mode APs, an active link takes you to a list of licensed access points. You cannot access a list of licensed clients and tags.	

Note

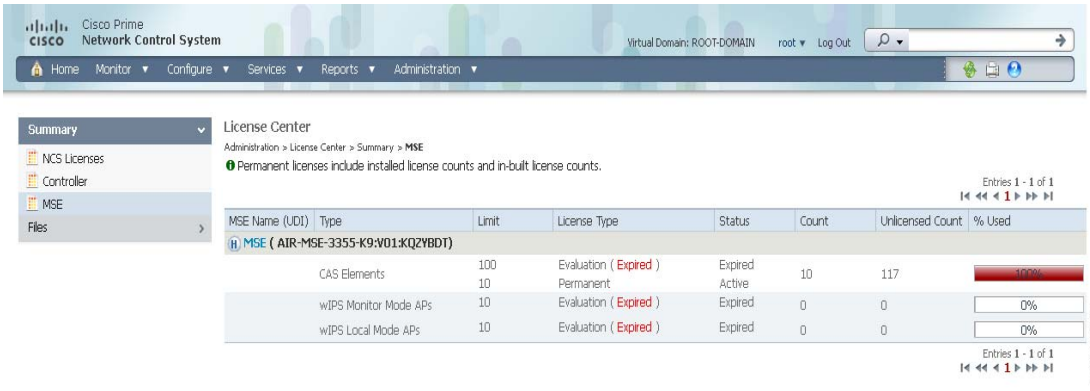
- When a license is deleted, the mobility services engine automatically restarts to load the new license limits.
- If Partner tag engine is up, then the MSE license information consists of information on tag licenses as well.

For more information on MSE licenses, see the "MSE License Overview" section on page 11-90.

Mobility Services Engine (MSE) License Summary

If you want to see more details about MSE licensing, choose **Summary > MSE** from the left sidebar menu. The License Center page appears (see Figure 15-56).

Figure 15-56 License Center Page



All licensed MSEs are listed in the following columns:

- MSE Name—Provides a link to the MSE license file list page.

Note The icon to the left of the MSE Name/UDI indicates whether the mobility services engine is low-end or high-end.
A high-end mobility services engine (3350) has a higher memory capacity and can track up to 18,000 clients and tags. A low-end mobility services engine (3310) can track up to 2000 clients and tags.

- Type—Specifies the type of MSE.

Note Under wIPS Monitor Mode APs or wIPS Local Mode APs, an active link takes you to a list of licensed access points. You cannot access a list of licensed clients or tags.

- Limit—Displays the total number of client elements licensed across MSEs.
- Count—Displays the number of client elements that are currently licensed across MSEs.
- Unlicensed Count—Displays the number of client elements that are not licensed.

Note wIPS service does not process the alarms generated from these unlicensed access points.

- % Used—Displays the percentage of clients used across all MSEs.
- License Type—The three different types of licenses are as follows:
  - Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
  - Evaluation—Licenses are non-node-locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license which has the fewest number of days until expiration is shown.

  - Extension—Licenses are node-locked and metered. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.
- Status
  - Active—License is installed and being used by a feature.
  - Inactive—License is installed but not being used by a feature.
  - Expired—License has expired.
  - Corrupted—License is corrupted.

For more information on MSE licenses, see the "MSE License Overview" section on page 11-90.

Managing NCS Licenses

If you choose Files > NCS Files from the left sidebar menu, you can manage the NCS licenses. This page displays the following information:

- Product Activation Key (PAK)
- Feature
- Access point limit
- Type

This section contains the following topics:

Adding a New NCS License File

To add a new NCS license file, follow these steps:

Step 1 In the License Center > Files > NCS Files page, click **Add**.

Step 2 In the Add a License File dialog box, enter or browse to the applicable license file.

Step 3 Once displayed in the License File text box, click **Upload**.

Deleting an NCS License File

To delete an NCS license file, follow these steps:

Step 1 In the License Center > Files > NCS Files page, select the check box of the NCS license file that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm the deletion.

Monitoring Controller Licenses

If you choose Files > Controller Files from the left sidebar menu, you can monitor the controller licenses.

Note The NCS does not directly manage controller licenses, rather it simply monitors the licenses. To manage the licenses you can use command-line interface, Web UI, or Cisco License Manager (CLM).

This page displays the following parameters:

- Controller Name
- Controller IP—The IP address of the controller.
- Feature—License features include wplus-ap-count, wplus, base-ap-count, and base.

  For every physical license installed, two license files display in the controller: a feature level license and an ap-count license. For example if you install a "WPlus 500" license on the controller, "wplus" and "wplus-ap-count" features display. There are always two of these features active at any one time that combine to enable the feature level (WPlus or Base) and the AP count.

  Note You can have both a WPlus and Base license, but only one can be active at any given time.

- AP Limit—The maximum capacity of access points allowed to join this controller.
- EULA status—Displays the status of the End User License Agreement and is either Accepted or Not Accepted.
- Comments—User entered comments when the license is installed.
- Type—The four different types of licenses are as follows:
  - Permanent—Licenses are node locked and have no usage period associated with them. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
  - Evaluation—Licenses are non-node locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node locked, their usage is recorded on the device. The number of days left displays for the evaluation license with the fewest number of remaining active license days.
  - Extension—Licenses are node locked and metered. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.
  - Grace Period—Licenses are node locked and metered. These licenses are issued by Cisco licensing portal as part of the permission ticket to rehost a license. They are installed on the device as part of the rehost operation, and you must accept a EULA as part of the rehost operation.

  Note Types other than Permanent display the number of days left until the license expires. Licenses not currently in use do not have their counts reduced until they become "In Use".

- Status

- In Use—The license level and the license are in use.
- Inactive—The license level is being used, but this license is not being used.
- Not In Use—The license level is not being used and this license is not currently recognized.
- Expired In Use—The license is being used, but is expired and will not be used upon next reboot.
- Expired Not In Use—The license has expired and can no longer be used.
- Count Consumed—The ap-count license is In Use.

Note If you need to filter the list of license files, you can enter a controller name, feature, or type and click **Go**.

Managing Mobility Services Engine (MSE) Licenses

If you choose Files > MSE Files from the left sidebar menu, you can manage the mobility services engine licenses.

This section contains the following topics:

- Registering Product Authorization Keys, page 15-142
- Installing Client and wIPS License Files, page 15-143
- Deleting a Mobility Services Engine License File, page 15-143

The page displays the mobility services engine licenses found and includes the following information:

Note Because tag licenses are added and managed using appropriate vendor applications, tag licenses are not displayed in this page. For more information, see the following URL: http://support.aeroscout.com.
Evaluation (demo) licenses are also not displayed.

Tag licenses are installed using the *AeroScout System Manager* only if the tags are tracked using Partner engine. Otherwise the tags are counted along with the CAS element license.

- MSE License File—Indicates the MSE license.
- MSE—Indicates the MSE name.
- Type—Indicates the type of mobility services engine (client elements, wIPS local mode or wIPS monitor mode access points).
- Limit—Displays the total number of client elements or wIPS monitor mode access points licensed across the mobility services engine.
- License Type—Permanent licenses are the only license types displayed on this page.
  - Permanent—Licenses are node locked and have no usage period associated with them. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.

Registering Product Authorization Keys

You receive a Product Authorization Key (PAK) when you order a client, wIPS, or tag license from Cisco. You must register the PAK to receive the license file for install on the mobility services engine. License files are e-mailed to you after successfully registering a PAK.

Client and wIPS PAKs are registered with Cisco.

Note Tag PAKs are registered with AeroScout. To register your tag PAK, go to this URL: http://www.aeroscout.com/content/support

To register a Product Authorization Key (PAK) to obtain a license file for install, follow these steps:

Step 1 Open a browser page and go to www.cisco.com/go/license.

Note You can also access this site by clicking the Product License Registration link located on the License Center page of the NCS.

Step 2 Enter the PAK and click **SUBMIT**.

Step 3 Verify the license purchase. Click **Continue** if correct. The licensee entry page appears.

Note If the license is incorrect, click the **TAC Service Request Tool** link to report the problem.

Step 4 At the Designate Licensee page, enter the mobility service engine UDI in the host ID text box. This is the mobility services engine on which the license is installed.

Note UDI information for a mobility services engine is found in the General Properties group box at Services > Mobility Services Engine > *Device Name* > *System*.

Step 5 Select the **Agreement** check box. Registrant information appears beneath the Agreement check box.

Modify information as necessary.

Note Ensure that the phone number does not include any characters in the string for the registrant and end user. For example, enter 408 555 1212 rather than 408.555.1212 or 408-555-1212.

Step 6 If registrant and end user are not the same person, select the **Licensee (End-User)** check box beneath registrant information and enter the end user information.

Step 7 Click **Continue**. A summary of entered data appears.

Step 8 At the Finish and Submit page, review registrant and end user data. Click **Edit Details** to correct information, if necessary.

Step 9 Click **Submit**. A confirmation page appears.

Installing Client and wIPS License Files

You can install CAS element licenses and wIPS licenses from the NCS.

Note Tag licenses are installed using the *AeroScout System Manager*. For additional information, see the following URL:
http://support.aeroscout.com.

To add a client or wIPS license to the NCS after registering the PAK, follow these steps:

Step 1 Choose **Administration > License Center**.

Step 2 From the left sidebar menu, choose **Files > MSE Files**.

Step 3 In the License Center > Files > MSE Files page, click **Add** to open the Add a License File dialog box.

Step 4 From the MSE Name drop-down list, choose the mobility services engine to which you want to add the license file.

Note Verify that the UDI of the selected mobility services engine matches the one you entered when registering the PAK.

Step 5 Enter the license file in the License File text box or browse to the applicable license file.

Step 6 Once displayed in the License File text box, click **Upload**. Newly added license appears in mobility services engine license file list.

Note A Context Aware Service (CAS) restarts if a client or tag license is installed; a wIPS service restarts if a wIPS license is installed.

Note Services must come up before attempting to add or delete another license.

Deleting a Mobility Services Engine License File

To delete a mobility services engine license file, follow these steps:

Step 1 In the License Center > Files > MSE Files page, select the check box of the mobility services engine license file that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm the deletion.

For more information on licenses, see the "Getting Started" section on page 2-1.

CHAPTER 11

NCS Services

This chapter contains the following sections:

Mobility Services

This section briefly describes the CAS, wIPS, and MSAP services that Cisco NCS supports and provides steps for mobility procedures that are common across all services.

CAS

Context-Aware Service (CAS) software allows a mobility services engine to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location, temperature, and availability from Cisco access points.

Note You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points. Licenses for tags and clients are offered independently. See the *Cisco 3350 Mobility Services Engine Release Note* at the following URL for details on tag and client licenses:

http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

wIPS

Cisco Adaptive Wireless IPS (wIPS) is an advanced approach to wireless threat detection and performance management. Cisco Adaptive wIPS combines network traffic analysis, network device and topology information, signature-based techniques and anomaly detection to deliver highly accurate and complete wireless threat prevention.

Note wIPS functionality is not supported for non-root partition users.

MSAP

Cisco Mobility Services Advertisement Protocol (MSAP)—The Cisco Mobility Services Advertisement Protocol (MSAP) provides functionality to deliver advertisements over Wi-Fi infrastructure. MSAP facilitates MSAP capable mobile devices to receive service advertisements. Once the mobile device receives the service advertisements, it can display their icons and data on its user interface, facilitating the process of users discovering what is available in their surroundings. In addition, MSAP can be used by the mobile devices that have been configured with a set of policies for establishing network connectivity. The MSAP provides requirements for clients and servers and describes the message exchanges between them.

This section contains the following topics:

Cisco Context-Aware Mobility Solution

The foundation of the CAM solution is the controller-based architecture of the CUWN. The CUWN contains the following primary components:

Cisco Prime NCS

With the NCS, network administrators have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and wired and wireless LAN systems management. Robust graphical interfaces make wired and wireless LAN deployment and operations simple and cost-effective. Detailed trending and analysis reports make NCS vital to ongoing network operations.

WLAN Controllers

The WLAN controllers are highly scalable and flexible platforms that enables system wide services for mission-critical wireless in medium to large-sized enterprises and campus environments. Designed for 802.11n performance and maximum scalability, the WLAN controllers offer enhanced uptime with the ability to simultaneously manage from 5000 access points to 250 access points; superior performance for reliable streaming video and toll quality voice; and improved fault recovery for a consistent mobility experience in the most demanding environments.

NCS supports the Cisco wireless controllers that help reduce the overall operational expense of Cisco Unified Networks by simplifying network deployment, operations, and management. The following WLAN controllers are supported in NCS:

- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 2500 Series Wireless Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless Controllers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless Services Module 2 (WiSM2) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless Controller on SRE for ISR G2 Routers
- Cisco Flex 7500 Series Wireless Controllers
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers

Access Points

The following access points are supported:

- Cisco Aironet 801, 802, 1000, 1040, 1100, 1130, 1140, 1200, 1230, 1240, 1250, 1260, 1310, 1500, 1524, 1552, 2600i, 2600e, 3500i, 3500e, 3500p, 3600i, and 3600e Series Lightweight Access Points.
- Cisco Aironet 1040, 1100, 1130, 1141, 1142, 1200, 1240, 1250, and 1260 Autonomous Access Points.

- Cisco 600 Series OfficeExtend Access Points.
- Cisco Aironet Access Points running Lightweight Access Point Protocol (LWAPP) or Control and Provisioning of Wireless Access Points (CAPWAP) protocol.

Cisco 3300 Series Mobility Services Engines

The Cisco 3300 Series Mobility Services Engine operates with CAS, which is a component of the CAM solution. There are three models of the mobility services engine:

- Cisco 33110 Mobility Services Engine
- Cisco 3350 Mobility Services Engine
- Cisco 3355 Mobility Services Engine
- Planning for and Configuring Context-Aware Software, page 11-95
- wIPS Planning and Configuring, page 11-97

Accessing Services

You can access the MSE installation guides as follows:

MSE 3350 Installation guide:

http://www.cisco.com/en/US/docs/wireless/mse/3350/quick/guide/mse_qsg.html

MSE 3310 Installation guide:

http://www.cisco.com/en/US/docs/wireless/mse/3310/quick/guide/MSE3310_GSG.html

MSE Services Co-Existence

With MSE 6.0 and later, you can enable multiple services (Context Aware and wIPS) to run concurrently. Before Version 6.0, mobility services engines only supported one active service at a time.

The following must be considered with co-existence of multiple services:

- Co-existence of services might be impacted by license enforcement. As long as the license is not expired, you can enable multiple services.

  Note Limits for individual services differ. For example, a low-end mobility services engine (MSE-3310) tracks a total of 2,000 CAS elements; a high-end mobility services engine (MSE-3350) tracks a total of 18,000 CAS elements.
  A low-end mobility services engine has a maximum limit of 2000 wIPS elements; a high-end mobility services engine has a maximum limit of 3000 wIPS elements.

- Expired evaluation licenses prevent the service from coming up.
- If a CAS license is added or removed, this process restarts all services on the mobility services engine including wIPS. If a wIPS license is added or removed, the process does not impact CAS; only wIPS restarts.
- Other services can be enabled in evaluation mode even if a permanent license for the maximum number of elements has been applied.

Whenever one of the services has been enabled to run with its maximum license, another service cannot be enabled to run concurrently because the capacity of the MSE is not sufficient to support both services concurrently. For example, on MSE-3310, if you install a wIPS license of 2000, then you cannot enable CAS to run concurrently. However, evaluation licenses are not subject to this limitation.

Note See the "Mobility Services Engine (MSE) License Information" section on page 15-136 for more information on mobility services engine licensing.

Viewing Current Mobility Services

To see a list of current Mobility Services, choose **Services > Mobility Services Engines**.

The Mobility Services Engines page provides the following information and features for each device:

- Device Name—User-assigned name for the mobility services engine. Click the device name to see and manage mobility services engine details. See the "Managing System Properties for a Mobility Services Engine" section on page 11-27" for more information.
- Device Type—Indicates the type of mobility services engine (for example, Cisco 3310 Mobility Services Engine). Indicates whether the device is a virtual appliance or not.
- IP Address—Indicates the IP address for the mobility services engine.
- Version—Indicates the version number of the mobility services engine.
- Reachability Status—Indicates whether or not the mobility services engine is reachable.
- Secondary Server—Indicates whether or not the secondary server is installed.
- Mobility Service:
  - Name—Indicates the name of the mobility service.
  - Admin Status—Indicates whether the mobility service is enabled or disabled.
  - Service Status—Indicates whether the mobility service is currently up or down.
- Select a command drop-down list:
  - Add Location Server
  - Add Mobility Services Engine—Contains Context-Aware Service and Cisco Adaptive Wireless IPS (wIPS) service.
  - Delete Service(s)
  - Synchronize Service
  - Synchronization History
  - Edit Configuration

Note Location and mobility services engine features of NCS do not support partitioning.

Adding a Mobility Services Engine

You can add MSE using the Add Mobility Services Engine dialog box in the Mobility Service page. In this dialog box, you can add licensing files, tracking parameters, and assign maps to MSE. If you launch the wizard with an existing MSE for configuration, then the Add MSE option appears as Edit MSE Details.

Tip To learn more about Cisco Adaptive wIPS features and functionality, go to Cisco.com to watch a multimedia presentation. Here you can find the learning modules for a variety of NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

Note The 1.0 release of NCS recognizes and supports MSE 3355 appropriately.

To add a Cisco 3300 series mobility services engine to NCS, follow these steps:

Step 1 Verify that you can ping the mobility service engine that you want to add from NCS.

Step 2 Choose **Services > Mobility Services Engines** to display the Mobility Services page.

Step 3 From the Select a command drop-down list, choose **Add Mobility Services Engine**, and click **Go**.

The Add Mobility Services Engine page appears.

Step 4 Enter the following information:

- Device Name—User-assigned name for the mobility services engine.
- IP Address—The IP address of the mobility service engine.

Note A mobility services engine is added only if a valid IP address is entered. The Device Name helps you distinguish between devices if you have multiple NCSs with multiple mobility services engines, but it is not considered when validating a mobility services engine.

- Contact Name (optional)—The mobility service engine administrator.
- Username—The default username is admin. This is the NCS communication username configured for MSE.
- Password—The default password is admin.This is the NCS communication password configured for MSE.

Note If you changed the username and password during the automatic installation script, enter those values here. If you did not change the default passwords, we recommend that you rerun the automatic installation script and change the username and password.

- HTTP—When enabled, HTTP is used for communication between the NCS and mobility services engine. By default, NCS uses HTTPS to communicate with MSE.

Note For HTTP communication with a mobility services engine, HTTP must be enabled explicitly on the mobility services engine.

- Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the mobility services engine.

  This option is applicable for network designs, wired switches, controllers, and event definitions. The existing location history data is retained, however you must use manual service assignments to perform any future location calculations.

Step 5 Click **Next**. The NCS automatically synchronizes the selected elements with the MSE.

After the synchronization, the MSE License Summary page appears. You can use the MSE License Summary page to install a license, add a license, remove a license, install an activation license, and install service license.

Configuring MSE Tracking and History Parameters

Step 6 After you enable services on the mobility services engine, the Select Tracking & History Parameters page appears.

Note If you skip configuring the tracking parameters, the default values are selected.

Step 7 You can select the clients that you want to keep track of by selecting the corresponding Tracking check box(es). The various tracking parameters are as follows:

- Wired Clients
- Wireless Clients
- Rogue Access Points
  - Exclude Adhoc Rogue APs
- Rogue Clients
- Interferers
- Active RFID Tags

Step 8 You can enable the history tracking of devices by selecting the corresponding devices check box(es). The different history parameters are as follows:

- Wired Stations
- Client Stations
- Rogue Access Points
- Rogue Clients
- Interferers
- Asset Tags

Step 9 Click Next to Assign Maps to the MSE.

Assigning Maps to the MSE

Note The Assigning Maps page is available only if you select CAS as one of the services to be enabled on the MSE.

Step 10 Once you configure MSE tracking and history parameters, the Assigning Maps page appears.

The Assign Maps page shows the following information:

- Map Name
- Type (building, floor, campus)
- Status

Step 11 You can see the required map type by selecting either All, Campus, Building, Floor Area, or Outdoor Area from the Filter option available on the page.

Step 12 To synchronize a map, select the **Name** check box and click **Synchronize**.

Upon synchronization of the network designs, the appropriate controllers that have APs assigned on a particular network design are synchronized with the MSE automatically.

Step 13 Click **Done** to save the MSE settings.

Deleting an MSE License File

To delete an MSE license file, follow these steps:

Step 1 Choose **Services > Mobility Service Engine**.

The Mobility Services page appears.

Step 2 Click **Device Name** to delete a license file for a particular service.

Step 3 From the Select a command drop-down list, choose Edit Configuration.

The Edit Mobility Services Engine dialog box appears.

Step 4 Click **Next** in the Edit Mobility Services Engine dialog box.

The MSE License Summary page appears.

Step 5 Choose the MSE license file that you want to delete in the MSE License Summary page.

Step 6 Click **Remove License**.

Step 7 Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the license.

Step 8 Click **Next** to enable services on the mobility services engine.

Deleting a Mobility Services Engine from Cisco NCS

To delete a mobility services engine from the NCS database, follow these steps:

Step 1 Choose **Services > Mobility Services Engine**.

The Mobility Services page appears.

Step 2 Select the mobility services engine(s) to be deleted by selecting the corresponding **Device Name** check box(es).

Step 3 From the Select a command drop-down list, choose **Delete Service(s)**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm that you want to delete the selected mobility services engine from the NCS database.

Step 6 Click **Cancel** to stop the deletion.

Registering Product Authorization Keys

You receive a product authorization key (PAK) when you order a CAS element, wIPS, or tag license from Cisco. You must register the PAK to receive the license file for installation on the mobility services engine. License files are e-mailed to you after successfully registering a PAK.

CAS element and wIPS PAKs are registered with Cisco.

Tag PAKs are registered with AeroScout.

Note If you do not have a PAK, you can use the sales order number to retrieve the PAK. See the "Retrieving a PAK" section on page 11-10 for more information.

To register for a Product Authorization Key (PAK) and to obtain a license file for install, follow these steps:

Step 1 Open a browser page and enter www.cisco.com/web/go/license/index.html.

Step 2 Enter the PAK, and click **SUBMIT**.

Step 3 Verify the license purchase. Click **Continue** if correct. The licensee entry page appears.

Note If the license is incorrect, click the **TAC Service Request Tool** URL to report the problem.

Step 4 In the Designate Licensee page, enter the UDI of the mobility services engine in the host ID text box. This is the mobility services engine on which the license is installed.

Note UDI information for a mobility services engine is found in the General Properties dashlet at **Services** > **Mobility Services Engine** > *Device Name* > *System*.

Step 5 Select the **Agreement** check box. Registrant information appears beneath the Agreement check box.

Modify information as necessary.

Note Ensure that the phone number does not include any characters in the string for the registrant and end user. For example, enter 408 555 1212 rather than 408.555.1212 or 408-555-1212.

Step 6 If the registrant and end user are not the same person, select the **Licensee (End-User)** check box beneath registrant information and enter the end user information.

Step 7 Click **Continue**. A summary of entered data appears.

Step 8 In the Finish and Submit page, review registrant and end-user data. Click **Edit Details** to correct any information, if necessary.

Step 9 Click **Submit**. A confirmation page appears.

Retrieving a PAK

If you do not have a PAK, you can use the sales order number to retrieve the PAK:

Step 1 Go to the Sales Order Status Tool at the following URL: http://tools.cisco.com/qtc/status/tool/action/LoadOrderQueryScreen.

Step 2 After logging in, choose **Sales Order (SO)** from the Type of Query drop-down list.

Step 3 Enter the sales order number in the Value text box.

Note The Date Submitted fields are not required for this inquiry.

Step 4 Select the **Show Serial Number** check box.

Step 5 Select the **Orders** radio button, if not already selected.

Step 6 Choose **Screen** from the Deliver through drop-down list.

Step 7 Click **Search**. Detailed information on the mobility services engine order appears.

Step 8 Click **Line 1. 1** in the table.

Step 9 In Product column (second line), copy the PAK number (starts with 3201J) that you want to register to obtain the license.

Installing Device and wIPS License Files

You can install device and wIPS licenses from NCS.

Note Tag licenses are installed using the *AeroScout System Manager*. To register your tag PAK, go to this URL: http://www.aeroscout.com/content/support

To add a client or wIPS license to NCS after registering the PAK, follow these steps:

Step 1 Choose **Administration > Licensing**.

Step 2 Choose **Files > MSE Files** (left pane).

Step 3 Click **Add**. A pop-up dialog box appears.

Step 4 Select **MSE Name**.

Note Verify that the UDI of the selected mobility services engine matches the one you entered when registering the PAK.

Step 5 Click **Choose File** to browse and to select the license file.

Step 6 Click **Upload**. The newly added license appears in the mobility services engine license file list.

Adding a Location Server

To add a location server, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 From the Select a command drop-down list, choose **Add Location Server**.

Step 3 Click **Go**.

Step 4 Enter the following information:

- Device Name
- IP Address
- Contact Name
- User Name
- Password
- Port
- HTTPS—When enabled, HTTPS is used for communication between the NCS and location server.

Step 5 Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the mobility services engine.

This option is applicable for network designs, wired switches, controllers, and event definitions. The existing location history data is retained, however, you must use manual service assignments to perform any future location calculations.

Step 6 Click **Save**.

Note After adding a location server, it must be synchronized with NCS. See the "Synchronizing Services" section on page 11-11 for more information.

Note Location and mobility services engine features of NCS do not support partitioning.

Synchronizing Services

This section describes how to synchronize Cisco wireless LAN controllers and NCS with mobility services engines and contains the following topics:

Keeping Mobility Services Engines Synchronized

This section describes how to synchronize NCS and mobility services engines manually and automatically.

After adding a mobility service engine to NCS, you can push (synchronize) network designs (campus, building, floor, and outdoor maps), event groups, controller information (name and IP address), or wired switches to the mobility services engine.

Note Be sure to verify software compatibility between the controller, NCS, and the mobility services engine before performing synchronization. See the latest mobility services engine release notes at the following URL: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

Note Communication between the mobility services engine, NCS, and the controller is in Coordinated Universal Time (UTC). Configuring NTP on each system provides devices with the UTC time. The mobility services engine and its associated controllers must be mapped to the same NTP server and the same NCS server. An NTP server is required to automatically synchronize time between the controller, NCS, and the mobility services engine.

Synchronizing NCS and a Mobility Services Engine

This section describes how to synchronize NCS and mobility services engines manually and smartly.

After adding a mobility services engine to NCS, you can synchronize network designs (campus, building, floor, and outdoor maps), controllers (name and IP address), specific Catalyst 3000 Series and 4000 switches, and event groups with the mobility services engine.

- Network Designs—Is a logical mapping of the physical placement of access points throughout facilities. A hierarchy of a single campus, the buildings that comprise that campus and the floors of each building constitute a single network design.
- Controllers—A selected controller that is associated and regularly exchanges location information with a mobility services engine. Regular synchronization ensures location accuracy.
- Event Groups—A group of predefined events that define triggers that generate an event. Regular synchronization ensures that the latest defined events are tracked.
- Wired Switches —Wired Catalyst switches that provide an interface to wired clients on the network. Regular synchronization ensures that location tracking of wired clients in the network is accurate.
  - The mobility services engine can be synchronized with Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports.

  - The mobility services engine can also be synchronized with the following Catalyst series switches 4000: WS-C4948, WS-C4948-10GE, ME-4924-10GE, WS-4928-10GE, WS-C4900M, WS-X4515, WS-X4516, WS-X4013+, WS-X4013+TS, WS-X4516-10GE, WS-X4013+10GE, WS-X45-SUP6-E, and WS-X45-SUP6-LE

- Third Party Elements—When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.
- Service Advertisements—MSAP provides service advertisements on the mobile devices. This shows the service advertisement that has synchronized with the MSE.

Note Be sure to verify software compatibility between the controller, Cisco NCS, and the mobility services engine before synchronizing. See the latest mobility services engine release notes at the following URL: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

Note Communication between the mobility services engine, NCS, and the controller is in Coordinated Universal Time (UTC). Configuring NTP on each system provides devices with the UTC time. The mobility services engine and its associated controllers must be mapped to the same NTP server and the same Cisco NCS server. An NTP server is required to automatically synchronize time between the controller, Cisco NCS, and the mobility services engine.

Synchronizing NCS Network Designs, Controllers, Wires Switches, or Group Events

To synchronize NCS network designs, controllers, wired switches, or event groups with the mobility services engine, follow these steps:

Step 1 Choose **Services > Synchronize Services**.

Step 2 Choose the appropriate menu option (Network Designs, Controllers, Wired Switches, or Event Groups).

Step 3 To assign a network design to a mobility services engine, from the left sidebar menu, choose **Network Designs**.

Step 4 Choose the maps that you want to be synchronized with the mobility services engine from the Type drop-down list.

Note Through 6.0, you can assign only up to a campus level to a mobility services engine. Beginning with 7.0 this option is granular to a floor level. For example, you can choose to assign floor1 to MSE 1, floor2 to MSE 2, and floor3 to MSE 3.

Step 5 Click **Change MSE Assignment**.

Step 6 Select the mobility services engine to which the maps are to be synchronized.

Note A network design might include a floor in a campus or a large campus with several buildings, each monitored by a different mobility services engine. Because of this, you might need to assign a single network design to multiple mobility services engines.

Step 7 Click **Synchronize** to update the mobility services engine(s) database(s).

When items are synchronized, a green two-arrow icon appears in the Sync. Status column for each synchronized entry.

You can use the same procedure to assign wired switches or event groups to a mobility services engine. See the "Synchronizing Controllers with Mobility Services Engines" section on page 11-14 for more information to assign a controller to a mobility services engine.

Step 8 Click **Cancel** to discard the changes made to the mobility services engine assignment and return to the Network Designs page.

You can also click **Reset** to undo the mobility services engine assignments.

Note Event groups can also be created by third-party applications. See the "Working with Third-Party Elements" section on page 11-15 for more information on Third-party application-created event groups.

Note You cannot unassign a network design and controller by clicking Change MSE Assignment if you are using the MSAP service because you defined the APs from the Service Advertisements tab. If you want to unassign, click **Service Advertisements** tab, click **Change MSE Assignment** and unselect the **service** check box if you do not want the elements to be associated.

To unassign a network design, controller, wired switch, or event group from a mobility services engine, follow these steps:

Step 1 On the respective tabs, click one or more elements, and click **Change MSE Assignment**. The Choose Mobility Services Engine dialog box appears.

Step 2 Unselect the **Mobility Services Engine** check box if you do not want the elements to be associated with that mobility services engine.

Step 3 Click **Save** to save the changes to the assignments.

Step 4 Click **Synchronize**. The Sync Status column appears blank.

Synchronizing Controllers with Mobility Services Engines

You can assign an MSE to any wireless controller on a per-service (CAS or wIPS) basis.

To assign an MSE service to wireless controllers, follow these steps:

Step 1 In the synchronization page, choose **Controllers**.

Step 2 Choose the controllers to be assigned to the mobility services engine.

Step 3 Click **Change MSE Assignment**.

Step 4 Choose the mobility services engine to which the controllers must be synchronized.

Step 5 Click either of the following in the dialog box:

- **Save**—Saves the mobility services engine assignment. The following message appears in the Messages column of the Controllers page:

To be assigned - Please synchronize.

- **Cancel**—Discards the changes to the mobility services engine assignment and returns to the Controllers page.

  You can also click **Reset** to undo the yellow button assignments.

Step 6 Click **Synchronize** to complete the synchronization process.

Step 7 Verify that the mobility services engine is communicating with each of the controllers for only the chosen service. This can be done by clicking the **NMSP status** link in the status page.

Note After Synchronizing a controller, verify that the timezone is set on the associated controller. See the "Setting and Verifying the Timezone on a Controller" section on page 11-16 for more information.

Note Controller names must be unique for synchronizing with a mobility services engine. If you have two controllers with the same name, only one is synchronized.

To unassign a network design, controller, wired switch, or event group from a mobility services engine, follow these steps:

Step 1 On the respective tabs, click one or more elements, and click **Change MSE Assignment**. The Choose Mobility Services Engine dialog box appears.

Step 2 Unselect the **Mobility Services Engine** check box if you do not want the elements to be associated with that mobility services engine.

Step 3 Click **Save** to save the changes to the assignments.

Step 4 Click **Synchronize**. A two-arrow icon appears in the Sync Status column.

Working with Third-Party Elements

When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.

To delete the elements or mark them as third-party elements, follow these steps:

Step 1 In the synchronization page, choose **Third Party Elements** from the left sidebar menu.

The Third Party Elements page appears.

Step 2 Choose one or more elements.

Step 3 Click one of the following buttons:

- **Delete Event Groups**—Deletes the selected event groups.
- **Mark as 3rd Party Event Group(s)**—Marks the selected event groups as third-party event groups.

Setting and Verifying the Timezone on a Controller

For controller releases 4.2 and later, if a mobility services engine (release 5.1 or greater) is installed in your network, it is mandatory that the time zone be set on the controller to ensure proper synchronization between the two systems.

Greenwich Mean Time (GMT) is used as the standard for setting the time zone system time of the controller.

You can automatically set the time zone during initial system setup of the controller or manually set it on a controller already installed in your network.

To manually set the time and time zone on an existing controller in your network using the CLI, follow these steps:

Step 1 Configure the current local time in GMT on the controller by entering the following commands:

```
(Cisco Controller) >config time manual 09/07/07 16:00:00
(Cisco Controller) >config end
```

Note When setting the time, the current local time is entered in terms of GMT and as a value between 00:00 and 24:00. For example, if it is 8 AM Pacific Standard Time (PST) in the US, you enter 16:00 (4 PM PST) as the PST time zone is 8 hours behind GMT.

Step 2 Verify that the current local time is set in terms of GMT by entering the following command:

```
(Cisco Controller) >show time
Time..................................... Fri Sep 7 16:00:02 2007
Timezone delta.............................. 0:0
```

Step 3 Set the local time zone for the system by entering the following commands:

Note When setting the time zone, you enter the time difference of the local current time zone with respect to GMT (+/-). For example, Pacific Standard Time (PST) in the United States (US) is 8 hours behind GMT (UTC) time. Therefore, it is entered as -8.

```
(Cisco Controller) >config time timezone -8
(Cisco Controller) >config end
```

Step 4 Verify that the controller shows the current local time with respect to the local time zone rather than in GMT by entering the following command:

```
(Cisco Controller) >show time
Time..................................... Fri Sep 7 08:00:26 2007
Timezone delta.............................. -8:0
```

Note The time zone delta parameter in the **show time** command shows the difference in time between the local time zone and GMT (8 hours). Before configuration, the parameter setting is 0.0.

Configuring Smart Mobility Services Engine Database Synchronization

Manual synchronization of NCS and mobility services engine databases provides immediate synchronization. However, future deployment changes (such as making changes to maps and access point positions), can yield incorrect location calculations and asset tracking until resynchronization reoccurs.

To prevent out-of-sync conditions, use NCS to carry out synchronization. This policy ensures that synchronization between NCS and mobility services engine databases is triggered periodically and any related alarms are cleared.

Any change to one or more of any synchronized components is automatically synchronized with the mobility services engine. For example, if a floor with access points is synchronized with a particular mobility services engine and then one access point is moved to a new location on the same floor or another floor which is also synchronized with the mobility services engine, then the changed location of the access point is automatically communicated.

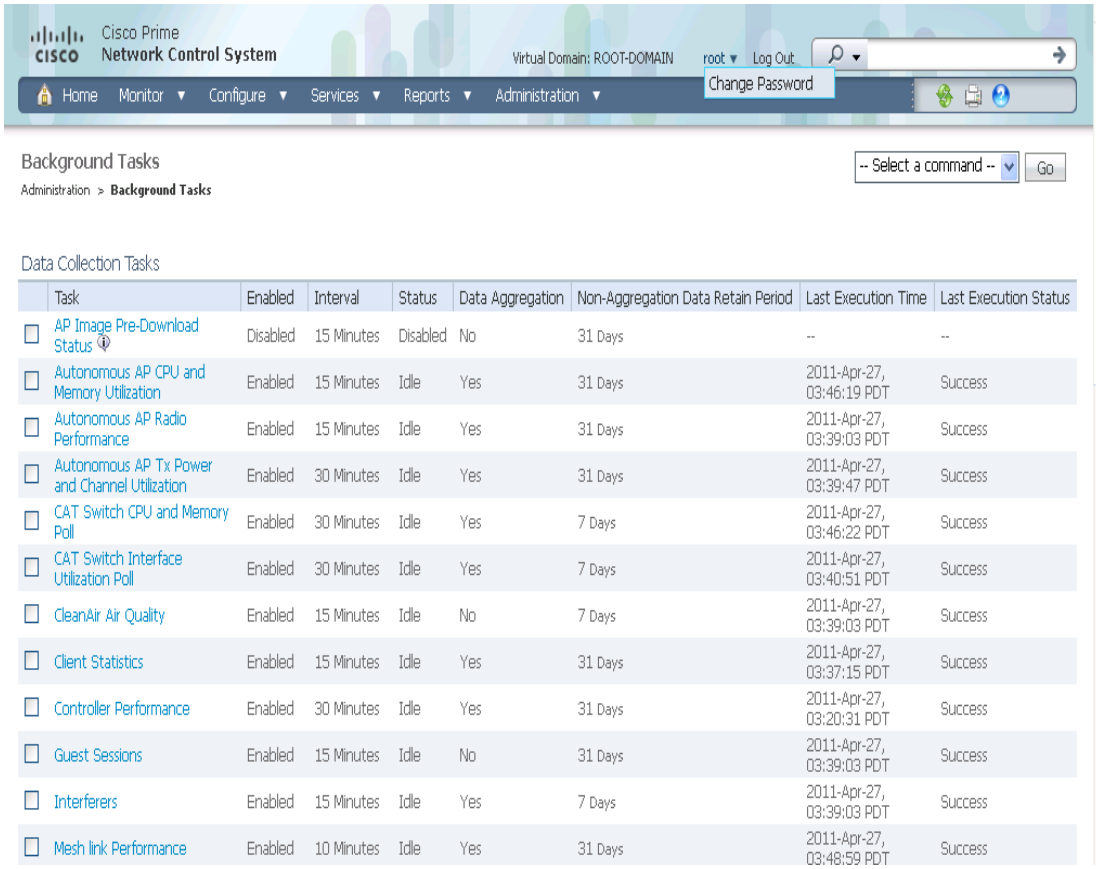
To further ensure that NCS and MSE are in sync, smart synchronization happens in the background.

To configure smart synchronization, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

The Background Tasks summary page appears (see Figure 11-1).

Figure 11-1 Administration > Background Tasks



Step 2 Select the **Mobility Service Synchronization** check box.

Step 3 Click the **Mobility Service Synchronization** link.

The Task > Mobility Service Synchronization page appears.

Step 4 To set the mobility services engine to send out-of-sync alerts, select the **Enabled** check box in the Out of Sync Alerts group box.

Step 5 To enable smart synchronization, select the Smart Synchronization **Enabled** check box.

Note

- Smart synchronization does not apply to elements (network designs, controllers, or event groups) that have not yet been assigned to a mobility services engine. However, out-of-sync alarms are still generated for these unassigned elements. For smart synchronization to apply to these elements, you need to manually assign them to a mobility services engine.
- When a mobility services engine is added to an NCS, the data in the NCS is always treated as the primary copy that is synchronized with the mobility services engine. All synchronized network designs, controllers, event groups and wired switches that are present in the mobility services engine and not in the NCS are removed automatically from mobility services engine.

Step 6 Enter the time interval in minutes that the smart synchronization is to be performed.

By default, smart-sync is disabled.

Step 7 Click **Submit**.

See the "Smart Controller Assignment and Selection Scenarios" section on page 11-19 for more information on smart controller assignment and selection scenarios.

Smart Controller Assignment and Selection Scenarios

Scenario 1

If a floor having at least one access point from a controller is chosen to be synchronized with the mobility services engine from the Network Designs section of the Synchronization page, then the controller to which that access point is connected is automatically selected to be assigned to the mobility services engine for CAS service.

Scenario 2

When at least one access point from a controller is placed on a floor that is synchronized with mobility services engine, the controller to which the access point is connected is automatically assigned to the same mobility services engine for CAS service.

Scenario 3

An access point is added to a floor and is assigned to an mobility services engine. If that access point is moved from controller A to controller B, then controller B is automatically synchronized to the mobility services engine.

Scenario 4

If all access points placed on a floor which is synchronized to the mobility services engine are deleted then that controller is automatically removed from mobility services engine assignment or unsynchronized.

Out-of-Sync Alarms

Out-of-sync alarms are of Minor severity (yellow) and are raised in response to the following conditions:

- Elements have been modified in NCS (the auto-sync policy pushes these elements).
- Elements have been modified in the mobility services engine.
- Elements except controllers exist in the mobility services engine database but not in NCS.
- Elements have not been assigned to any mobility services engine (the auto-sync policy does not apply).

Out-of-sync alarms are cleared when the following occurs:

- The mobility services engine is deleted

Note When you delete a mobility services engine, the out-of-sync alarms for that system is also deleted. In addition, if you delete the last available mobility services engine, the alarms for "elements not assigned to any server" are also deleted.

- Elements are synchronized manually or automatically
- User manually clears the alarms (although the alarms might reappear the future when the scheduled task is next executed)

Note By default, out-of-sync alarms are enabled. You can disable them in NCS by choosing **Administration > Scheduled Tasks**, clicking **Mobility Service Synchronization**, unselecting the **Auto Synchronization** check box, and clicking **Submit**.

Viewing Mobility Services Engine Synchronization Status

You can use the Synchronize Servers command in NCS to view the status of network design, controller, and event group synchronization with a mobility services engine.

To view synchronization status, follow these steps:

Step 1 Choose **Services > Synchronize Services**.

Step 2 Choose the applicable menu option (**Network Designs**, **Controllers**, or **Event Groups**).

For each of the elements, the Sync. Status column shows the synchronization status. A green two-arrow icon indicates that its corresponding element is synchronized with the specified server such as a mobility services engine. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a given server.

Note A green two-arrow icon does not indicate the NMSP connection status for a controller.

You can also view the synchronization status and assign or unassign from the campus view and building view along with floor view.

To access this page, choose **Monitor > Maps > System Campus >** *Building* **>** *Floor*

where *Building* is the building within the campus and *Floor* is a specific floor in that campus building.

The MSE Assignment option on the left sidebar menu shows which mobility services engine the floor is currently assigned to. You can also change mobility services engine assignment from this page.

Viewing Synchronization History

You can use the Synchronization History command in NCS to view the synchronization history for the last 30 days for a mobility services engine. This is especially useful when automatic synchronization is enabled as alarms are automatically cleared. Synchronization History provides a summary of those cleared alarms.

To view synchronization history, choose **Services > Synchronization History** and click the column headers to sort the entries.

Viewing Notification Statistics

You can view the notification statistics for a specific mobility services engine. To view the Notification Statistics for a specific mobility services engine:

Choose **Services > Mobility Services >** *MSE-name* **> Context Aware Service > Notification Statistics**.

where *MSE-name* is the name of a mobility services engine.

Table 11-1 describes the fields in the Notification statistics page.

Table 11-1 Notification Statistics fields

Field	Description
Summary	
Destinations	
Total	Total destination count.
Unreachable	Unreachable destination count.
Notification Statistics Summary	
Track Definition Status	Status of the track definition. Track notification status can be either Enabled or Disabled.
Track Definition	Track definition can be either Northbound or CAS event notification.
Destination IP Address	The destination IP address to which the notifications are sent.
Destination Port	The destination port to which the notifications are sent.
Destination Type	The type of the destination. Example: SOAP_XML
Destination Status	Status of the destination device. The status is either Up or Down.
Last Sent	The date and time at which the last notification was sent to the destination device.
Last Failed	The date and time at which the notification failed.
Total Count	The total count of notifications sent to the destination. Click the count link to view the notification statistics details of the destination device.

Configuring High Availability

The mobility services engine is a platform for hosting multiple mobility applications. Every active MSE is backed up by another inactive instance. The main component of high availability system is the health monitor. The health monitor configures, manager, and monitors the high availability setup. Heartbeat is maintained between the primary and secondary MSE. Health monitor is responsible for setting up database, file replication, and monitoring the application. When the primary MSE fails and secondary takes over, the virtual address of the primary MSE is switched transparently.

The following are some information about the architecture:

- Every active primary MSE is backed up by another inactive instance. The secondary MSE becomes active only after the failover procedure is initiated.
- The failover procedure can be manual or automatic.
- One secondary MSE can support two primary MSEs.
- There is one software and database instance for each registered primary MSE.

This section provides information on the following:

Pairing Matrix

The Table 11-13 gives information on the pairing matrix.

Table 11-2 Pairing Matrix

	Secondary Server Type							
Primary Server Type		3310	3350	3355	VA-2	VA-3	VA-4	VA-5
	3310	Y	Y	Y	N	N	N	N
	3350	N	Y	Y	N	N	N	N
	3355	N	Y	Y	N	N	N	N
	VA-2	N	N	N	Y	Y	Y	Y
	VA-3	N	N	N	N	Y	Y	Y
	VA-4	N	N	N	N	N	Y	Y
	VA-5	N	N	N	N	N	N	Y

The Table 11-13 gives information on the pairing matrix.

Table 11-3 Pairing Matrix

Secondary Server	**Primary Server**
3310	N:1 not supported
3350	Two 3310 servers are supported
3355	Two 3310 servers are supported
3355	Two 3350 servers are supported
3355	One 3310 and one 3350 are supported

Guidelines and Limitations for High Availability

- Both the health monitor IP and Virtual IP should be accessible from NCS.
- Always health monitor IP and virtual IP should be different.
- You can use either manual or automatic failover.
- You can use either manual or automatic failback.
- Both primary and secondary MSE should be on the same software version.

Failover Scenario for High Availability

When a failure of a primary MSE is detected, the following events take place:

Note One secondary MSE can back two primary devices.

- The primary MSE is confirmed as non-functioning (hardware fail, network fail, and so on) by the health monitor on the secondary MSE.
- If automatic failover has been enabled, MSE is started on the secondary immediately and uses the corresponding database of the primary MSE.
- Failback is invoked and the primary MSE takes back all the operations.
- The result of the failover operation is indicated as an event in the Health Monitor UI, and critical alarm is sent to the administrator.

Failback

When the primary MSE is restored to its normal state if the secondary MSE is already failing over for the primary, then failback can be invoked.

Failback can occur only if the secondary MSE is in one of the following states for the primary instance:

- The secondary MSE is actually failing over for the primary MSE.
- If manual failover is configured but the administrator did not invoke it.
- The primary failed but the secondary MSE cannot take over because it has encountered some errors or it is failing over another primary MSE.
- Failback can occur only if the administrator starts up the failed primary MSE.

HA Licensing

There is no separate license required to set up an MSE HA system.

Configuring High Availability on the MSE

Configuring high availability on the MSE involves the following two steps:

- During the installation of the MSE software, you must perform certain configurations using the command-line client.
- Pair up the primary and secondary MSE from the NCS UI.

Note If you do not want high availability support and if you are upgrading from an older release, you can continue to use the old IP address for the MSE. If you want to set up high availability, then you must configure the health monitor IP address. The health monitor then becomes a virtual IP address.

Note By default, all MSEs are configured as primary.

To configure high availability on the primary MSE, follow these steps:

Step 1 Ensure that the network connectivity between the primary and secondary is functioning and that all the necessary ports are open.

Step 2 Install the correct version of MSE on the primary MSE.

Step 3 Make sure that the same MSE release version that is loaded on the other primary MSE and secondary MSE is also loaded on the new primary MSE.

Step 4 On the intended primary MSE, enter the following command:

```
/opt/mse/setup/setup.sh
----------------------------------------------------------------
Welcome to the appliance setup.
Please enter the requested information.  At any prompt,
enter ^ to go back to the previous prompt. You may exit at
any time by typing <Ctrl+C>.
You will be prompted to choose whether you wish to configure a
parameter, skip it, or reset it to its initial default value.
Skipping a parameter will leave it unchanged from its current
value.
Changes made will only be applied to the system once all the
information is entered and verified.
----------------------------------------------------------------
```

Step 5 Configure the hostname:

```
Current hostname=[mse]
Configure hostname? (Y)es/(S)kip/(U)se default [Skip]:
```

The hostname should be a unique name that can identify the device on the network. The hostname should start with a letter, end with a letter or number, and contain only letters, numbers, and dashes.

Step 6 Configure the domain name:

Enter a domain name for the network domain to which the device belongs. The domain name should start with a letter, and it should end with a valid domain name suffix such as *.com*. It must contain only letters, numbers, dashes, and dots.

```
Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]:
```

Step 7 Configure the HA role:

```
Current role=[Primary]
Configure High Availability?  (Y)es/(S)kip/(U)se default [Skip]:
High availability role for this MSE (Primary/Secondary):
Select role [1 for Primary, 2 for Secondary] [1]: 1
Health monitor interface holds physical IP address of this MSE server.
```

```
This IP address is used by Secondary, Primary MSE servers and NCS to communicate among
themselves
Select Health Monitor Interface [eth0/eth1] [eth0]:eth0
------------------------------------------------------------------
Direct connect configuration facilitates use of a direct cable connection between the
primary and secondary MSE servers.
This can help reduce latencies in heartbeat response times, data replication and failure
detection times.
Please choose a network interface that you wish to use for direct connect. You should
appropriately configure the respective interfaces.
\"none\" implies you do not wish to use direct connect configuration.
------------------------------------------------------------------
```

Step 8 Configure Ethernet interface parameters:

```
Select direct connect interface [eth0/eth1/none] [none]: eth0
Enter a Virtual IP address for first this primary MSE server:
Enter Virtual IP address [172.31.255.255]:
Enter the network mask for IP address 172.31.255.255.
Enter network mask [255.255.255.0]:
Current IP address=[172.31.255.255]
Current eth0 netmask=[255.255.255.0]
Current gateway address=[172.31.255.256
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

Step 9 When prompted for "eth1" interface parameters, enter Skip to proceed to the next step. A second NIC is not required for operation:

```
Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

Follow Step 10 through Step 13 to configure the secondary MSE.

Step 10 Configure the hostname for the secondary MSE:

```
Current hostname=[]
Configure hostname? (Y)es/(S)kip/(U)se default [Skip]:
```

Step 11 Configure the domain name:

```
Current domain=
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]:
```

Step 12 Configure the HA role:

```
Current role=[Primary]
Configure High Availability?  (Y)es/(S)kip/(U)se default [Skip]:
High availability role for this MSE (Primary/Secondary)
Select role [1 for Primary, 2 for Secondary] [1]: 2
Health monitor interface holds physical IP address of this MSE server.
This IP address is used by Secondary, Primary MSE servers and NCS to communicate among
themselves
Select Health Monitor Interface [eth0/eth1] [eth0]:[eth0/eth1]
------------------------------------------------------------------
Direct connect configuration facilitates use of a direct cable connection between the
primary and secondary MSE servers.
This can help reduce latencies in heartbeat response times, data replication and failure
detection times.
Please choose a network interface that you wish to use for direct connect. You should
appropriately configure the respective interfaces.
\"none\" implies you do not wish to use direct connect configuration.
------------------------------------------------------------------
```

Step 13 Configure ethernet interface parameters:

```
Select direct connect interface [eth0/eth1/none] [none]: eth1
Enter a Virtual IP address for first this primary MSE server
Enter Virtual IP address [172.19.35.61]:
Enter the network mask for IP address 172.19.35.61:
Enter network mask [255.255.254.0]:
Current IP address=[172.19.35.127]
Current eth0 netmask=[255.255.254.0]
Current gateway address=[172.19.34.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

Step 14 Once you have configured both the primary MSE and secondary MSE, the NCS UI should be used to set up a pairing between the primary and secondary MSE.

Step 15 Once the primary MSE is added successfully, choose **Services > High Availability** or click the primary MSE device in the **Services > Mobility Services Engine** page, and choose **HA Configuration > Service High Availability** from the left sidebar menu.

The HA Configuration page appears.

Step 16 Enter the secondary device name with which you want to pair the primary MSE.

Step 17 Enter the secondary IP address which is the health monitor IP address of the secondary MSE.

Step 18 Enter the secondary password. This is the NCS communication password configured on the MSE.

Step 19 Specify the failover type. You can choose either Manual or Automatic from the Failover Type drop-down list. After 10 seconds, the system fails over. The secondary server waits for a maximum of 10 seconds for the next heartbeat from the primary server. If it does not get the heartbeat in 10 seconds, it declares a failure.

Step 20 Specify the failback type by choosing either **Manual** or **Automatic** from the Failback Type drop-down list.

Step 21 Specify the Long Failover Wait in seconds.

After 10 seconds, the system fails over. The maximum failover wait is 2 seconds.

Step 22 Click **Save**.

The pairing and the synchronization happens automatically.

Step 23 To check whether the heartbeat is received from the primary MSE or not, choose **Services > Mobility Services Engine**, and click **Device Name** to view the configured parameters.

Step 24 Choose **HA Configuration > Service High Availability** from the left sidebar menu.

Check whether the heartbeat is received from the primary MSE or not.

Viewing Configured Parameters for High Availability

To view the configured parameters for high availability, follow these steps:

Step 1 Choose **Services > High Availability**.

Step 2 Click **Device Name** to view its configured parameters.

The HA configuration page appears.

Step 3 Choose **Services High Availability > HA Configuration** from the left sidebar menu. The HA Configuration page shows the following information:

- Primary Health Monitor IP
- Secondary Device Name
- Secondary IP Address
- Secondary Password
- Failover Type
- Failback Type
- Long Failover Wait

Viewing High Availability Status

To view the high availability status, follow these steps:

Step 1 Choose **Services > High Availability**.

Step 2 Click **Device Name** to view the desired status.

The HA Configuration page appears.

Step 3 Choose **Services High Availability > HA Status** from the left sidebar menu. The HA Configuration page shows the following information:

- Current high Availability Status
  - Status—Shows whether the primary and secondary MSE instances are correctly synchronized or not.
  - Heartbeats—Shows whether the heartbeat is received from the primary MSE or not
  - Data Replication—shows whether the data replication between the primary and secondary databases is happening or not.
  - Mean Heartbeat Response Time—shows the mean heartbeat response time between the primary and secondary MSE instance.
- Event Log—Shows all the events generated by the MSE. It shows the last 20 events.

Managing System Properties for a Mobility Services Engine

You can manage the system properties of a mobility services engine using the NCS. This section describes the various system properties of a mobility services engine and contains the following topics:

- Managing Maintenance for Mobility Services, page 11-42

Editing General Properties for a Mobility Services Engine

You can use NCS to edit the general properties of a mobility services engine registered in the NCS database. General properties include contact name, username, password, and HTTP.

To edit the general properties of a mobility services engine, follow these steps:

Step 1 Choose **Services > Mobility Services** to display the Mobility Services page.

Step 2 Click the name of the mobility services engine that you want to edit. The General Properties page (with a General tab and Performance tab) opens.

On the General tab, the following read-only server details appear:

- Device Name
- Device Type
- Device UDI

Note For licensing, the Device UID is the string between double quote characters (including spaces in the end, if any). Exclude the double quote characters using copy-paste.

- Version
- Start Time
- IP Address

Step 3 In the General Properties page, modify the following Server Details as necessary:

- Contact Name—Enter a contact name for the mobility service.
- Username—Enter the log in username for the NCS server that manages the mobility service.
- Password—Enter the log in password for the NCS server that manages the mobility service.
- HTTP—Select the **HTTP enable** check box to enable HTTP.

Note When you have a non-default port or HTTPS turned on, you must pass the correct information along with the command. For example, *getserverinfo* must include *-port <<port>> -protocol <<HTTP/HTTPS>>*. Similarly, for stopping the server, *stoplocserver -port <<port>> -protocol <HTTP/HTTPS>>*.

- Legacy Port—8001
- Legacy HTTPS—Select the check box to enable the legacy HTTPS.
- Delete synchronized service assignments and enable synchronization—Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the mobility services engine. This option shows up only if the delete synchronized service assignments check box was unselected while adding a mobility services engine.

Note NCS always uses HTTPS to communicate with a mobility services engine.

Note The following tcp ports are in use on the MSE in Release 6.0: tcp 22: MSE SSH port, tcp 80: MSE HTTP port, tcp 443: MSE HTTPS port, tcp 1411: AeroScout, tcp 1999: AeroScout internal port, tcp 4096: AeroScout notifications port, tcp 5900X: AeroScout (X can vary from 1 to 10), and tcp 8001: Legacy port. Used for location APIs.

Note The following udp ports are in use on the MSE in Release 6.0: udp 123: NTPD port (open after NTP configuration), udp 162: AeroScout SNMP, udp/tcp 4000X: AeroScout proxy (X can vary from 1 to 5), udp 12091: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints), udp 12092: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints), udp 32768: Location internal port, udp 32769: AeroScout internal port, and udp 37008: AeroScout internal port.

Step 4 In the Mobility Services dialog box, select the **Admin Status** check box to enable the applicable (Context Aware Service or wIPS).

If you select Context Aware Service then you must select a location engine to perform location calculation.

Choose either of the following:

- Cisco Tag Engine

  or

- Partner Tag Engine

Note With MSE 6.0, you can enable multiple services (CAS and wIPS) simultaneously. Before Version 6.0, mobility services engines can only supported one active service at a time.

The Mobility Services dialog box also shows the following:

- Service Name
- Service Version
- Service Status
- License Type

Note Use the **Click here** link to view mobility services engine licensing details. See the "Mobility Services Engine (MSE) License Information" section on page 15-136 for more information.

Step 5 Click **Save** to update the NCS and mobility service databases.

Note Use the **Click here** link to view mobility services engine licensing details.

Step 6 Click the **Performance** tab to view a graph of CPU and memory utilization percentages.

Editing NMSP Parameters for a Mobility Services Engine

Network Mobility Services Protocol (NMSP) manages communication between the mobility service and the controller. Transport of telemetry, emergency, and RSSI values between the mobility service and the controller is managed by this protocol.

Note

- The NMSP parameter is supported in mobility services installed with Release 3.0 through 7.0.105.0. It is not supported on releases later than 7.0.105.0.
- NMSP replaces the LOCP term introduced in release 3.0.
- Telemetry and emergency information is only seen on controllers and NCS installed with release 4.1 software or greater and on mobility services running release 3.0 or later software.
- The TCP port (16113) that the controller and mobility service communicate over must be open (not blocked) on any firewall that exists between the controller and mobility service for NMSP to function.

The NMSP Parameters dialog box of NCS enables you to modify NMSP parameters such as echo and neighbor dead intervals as well as response and retransmit periods.

To configure NMSP parameters, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine whose properties you want to edit.

Step 3 From the left sidebar menu, choose **System > NMSP Parameters**.

Step 4 Modify the NMSP parameters as appropriate.

Note No change in the default parameter values is recommended unless the network is experiencing slow response or excessive latency.

NMSP parameters include the following:

- Echo Interval—Defines how frequently an echo request is sent from a mobility service to a controller. The default value is 15 seconds. Allowed values range from 1 to 120 seconds.

  Note If a network is experiencing slow response, you can increase the values of the echo interval, neighbor dead interval and the response timeout values to limit the number of failed echo acknowledgements.

- Neighbor Dead Interval—The number of seconds that the mobility service waits for a successful echo response from the controller before declaring the neighbor dead. This timer begins when the echo request is sent.

  The default values is 30 seconds. Allowed values range from 1 to 240 seconds.

  Note This value must be at least two times the echo interval value.

- Response Timeout—Indicates how long the mobility service waits before considering the pending request as timed out. The default value is one second. Minimum value is one (1). There is no maximum value.
- Retransmit Interval—Interval of time that the mobility service waits between notification of a response time out and initiation of a request retransmission. The default setting is 3 seconds. Allowed values range from 1 to 120 seconds.
- Maximum Retransmits—Defines the maximum number of retransmits that are done in the absence of a response to any request. The default setting is 5. Allowed minimum value is zero (0). There is no maximum value.

Step 5 Click ***Save*** to update the NCS and mobility service databases.

Viewing Active Session Details for a Mobility Services Engine

The Active Sessions dialog box of NCS enables you to view active user sessions on the mobility services engine.

To view active user sessions, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility service.

Step 3 From the left sidebar menu, choose **System > Active Sessions**.

NCS shows a list of active mobility service sessions. For every session, NCS shows the following information:

- Session identifier
- IP address from which the mobility service is accessed
- Username of the connected user
- Date and time when the session started
- Date and time when the mobility service was last accessed
- How long the session was idle since the last access

Viewing and Adding Trap Destinations for a Mobility Services Engine

The Trap Destinations dialog box of NCS enables you to specify which NCS or Cisco Security Monitoring, Analysis, and Response System (CS-MARS) network management platform is the recipient of SNMP traps generated by the mobility services engine.

To view or manage trap destination for a mobility services engine, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility service.

Step 3 From the left sidebar menu, choose **System > Trap Destinations**.

NCS shows a list of current trap destinations including the following information:

- IP address
- Port number
- Community
- Destination type
- SNMP Version

Use the Select a command drop-down list to add or delete a trap destination.

To add a trap destination, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility service.

Step 3 From the left sidebar menu, choose **System > Trap Destinations**.

Step 4 Choose **Add Trap Destination** from the command drop-down list.

The New Trap Destination page appears.

Step 5 Enter the following details (see Table 11-4).

Table 11-4 Add Trap Destination page

Field	Description
IP Address	IP address for the trap destination
Port Number	Port number for the trap destination. The default port number is 162.
Destination Type	This field is not editable and has a value of **Other**.
SNMP Version	Select either v2c or v3.
The following set of fields appear only if you select v3 as the SNMP version.	
User Name	Username for the SNMP Version 3.
Security Name	Security name for the SNMP Version 3.
Authentication Type	Select one of the following: HMAC-MD5 HMAC-SHA
Authentication Password	Authentication password for the SNMP Version 3.
Privacy Type	Select one of the following: CBC-DES CFB-AES-128 CFB-AES-192 CFB-AES-256
Privacy Password	Privacy password for the SNMP Version 3.

Step 6 Click **Save** to save the changes or **Cancel** to discard the changes.

Editing Advanced Parameters for a Mobility Services Engine

The Advanced Parameters dialog box of NCS enables you to set the number of days events are kept, set session time out values, set an absent data interval cleanup interval, and enable or disable Advanced Debug.

Note You can use NCS to modify troubleshooting parameters for a mobility services engine.

To edit advanced parameters for a mobility services engine, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility service whose properties you want to edit.

Step 3 From the left sidebar menu, choose **System > Advanced Parameters**.

Step 4 View or modify the advanced parameters as necessary.

- General Information
- Advanced Parameters

Caution Because advanced debugging slows the mobility service down, enable advanced debugging only under the guidance of Cisco TAC personnel.

  - Number of Days to keep Events—Enter the number of days to keep logs. Change this value as required for monitoring and troubleshooting.
  - Session Timeout—Enter the number of minutes before a session times out. Change this value as required for monitoring and troubleshooting. Currently this option appears dimmed.
- Cisco UDI
  - Product Identifier (PID)—The Product ID of the mobility services engine.
  - Version Identifier (VID)—The version number of the mobility services engine.
  - Serial Number (SN)—Serial number of the mobility services engine.
- Advanced Commands
  - Reboot Hardware—Click to reboot the mobility service hardware. See the "Rebooting the Mobility Services Engine Hardware" section on page 11-34 for more information.
  - Shutdown Hardware—Click to turn off the mobility service hardware. See the "Shutting Down the Mobility Services Engine Hardware" section on page 11-34 for more information.
  - Clear Database—Click to clear the mobility services database. See the "Clearing the Mobility Services Engine Database" section on page 11-34 for more information. Unselect the **Retain current service assignments in NCS** check box to remove all existing service assignments from NCS and MSE. The resources have to be reassigned from **Services > Synchronize Services** page. This option is selected by default.

Step 5 Click **Save** to update the NCS and mobility service databases.

Rebooting the Mobility Services Engine Hardware

If you need to restart a mobility services engine, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to reboot.

Step 3 Click **System**.

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands dialog box, click **Reboot Hardware**.

Step 6 Click **OK** to confirm that you want to reboot the mobility services engine hardware.

The rebooting process takes a few minutes to complete.

Shutting Down the Mobility Services Engine Hardware

If you need to shut down a mobility services engine, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to shut down.

Step 3 Click **System**.

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands dialog box, click **Shutdown Hardware**.

Step 6 Click **OK** to confirm that you want to shut down the mobility services engine.

Clearing the Mobility Services Engine Database

To clear a mobility services engine configuration and restore its factory defaults, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine you want to configure.

Step 3 Click **System**.

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands dialog box, unselect the **Retain current service assignments in NCS** check box to remove all existing service assignments from NCS and MSE.

The resources have to be reassigned in the Services > Synchronize Services page. By default, this option is selected.

Step 6 In the Advanced Commands dialog box, click **Clear Database**.

Step 7 Click **OK** to clear the mobility services engine database.

Working with Logs

This section describes how to configure logging options and how to download log files and contains the following topics:

Configuring Logging Options

You can use NCS to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to configure.

Step 3 Choose **System > Logs**. The advanced parameters for the selected mobility services engine appear.

Step 4 Choose the appropriate options from the Logging Level drop-down list.

There are four logging options: Off, Error, Information, and Trace.

All log records with a log level of Error or preceding are logged to a new error log file locserver-error-%u-%g.log. This is an additional log file maintained along with the location server locserver-%u-%g.log log file. The error log file consists of logs of Error level along with their context information. The contextual information consists of 25 log records prior to the error. You can maintain upto 10 error log files. The maximum size allowed for each log file is 10 MB.

Caution Use Error and Trace only when directed to perform so by Cisco TAC personnel.

Step 5 Select the **Enabled** check box next to each element listed in that section to begin logging its events.

Step 6 Select the **Enable** check box in the Advanced Parameters dialog box to enable advanced debugging. By default, this option is disabled.

Step 7 To download log files from the server, click **Download Logs**. See the "Downloading Mobility Services Engine Log Files" section on page 11-36 for more information.

Step 8 In the Log File group box, enter the following:

- The number of log files to be maintained in the mobility services engine. You can maintain a minimum of 5 log files and a maximum of 20 log files in the mobility services engine.
- The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.

Step 9 In the MAC Address Based Logging group box, do the following:

- Select the **Enable** check box to enable MAC address logging. By default, this option is disabled.
- Add one or more MAC addresses for which you want to enable logging. You can also remove MAC addresses that you have already added by selecting the MAC address from the list and clicking **Remove**.

See the "MAC Address-based Logging" section on page 11-36 for more information on MAC Address-based logging.

Step 10 Click **Save** to apply your changes.

MAC Address-based Logging

This feature allows you to create log files that are specific to an entity whose MAC address is specified. The log files are created in the locserver directory under the following path:

/opt/mse/logs/locserver

A maximum of 5 MAC addresses can be logged at a time. The Log file format for MAC address aa:bb:cc:dd:ee:ff is macaddress-debug-aa-bb-cc-dd-ee-ff.log

You can create a maximum of two log files for a MAC Address. The two log files might consist of one main and one backup or rollover log file.

The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC Address. The MAC log files that are not updated for more than 24 hours are pruned.

Downloading Mobility Services Engine Log Files

If you need to analyze mobility services engine log files, you can use NCS to download them to your system. NCS downloads a zip file containing the log files.

To download a zip file containing the log files, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine to view its status.

Step 3 From the left sidebar menu, choose **Logs**.

Step 4 Click **Download Logs**.

Step 5 Follow the instructions in the File Download dialog box to open the file or save the zip file to your system.

Managing User and Group Accounts for a Mobility Services Engine

This section describes how to configure and manage users and groups on the mobility services engine.

This section describes how to add, delete, and edit users for a mobility services engine and contains the following topics:

- Adding Users for a Mobility Services Engine, page 11-37
- Deleting Users, page 11-37
- Editing User Properties, page 11-38

Note See the "Viewing Active Session Details for a Mobility Services Engine" section on page 11-31 for information on viewing active sessions for each user.

- Managing Group Accounts—This section describes how to add, delete, and edit user groups for a mobility services engine and contains the following topics:
  - Adding User Groups, page 11-38
  - Deleting User Groups, page 11-38
  - Editing Group User Permissions, page 11-39

Adding Users for a Mobility Services Engine

To add a users to a mobility services engine, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the device name of the mobility services engine that you want to edit.

Step 3 From the left sidebar menu, choose **Systems > Accounts > Users**.

Step 4 From the Select a command drop-down list, choose **Add User**.

Step 5 Click **Go**.

Step 6 Enter the username in the Username text box.

Step 7 Enter a password in the Password text box.

Step 8 Enter the name of the group to which the user belongs in the Group Name text box.

Step 9 Choose a permission level from the Permission drop-down list.

There are three permission levels to choose from: Read Access, Write Access, and Full Access (required for NCS to access a mobility services engine).

Caution Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with read access, that user is unable to configure mobility services engine settings.

Step 10 Click **Save** to add the new user to the mobility services engine.

Deleting Users

To delete a user from a mobility services engine, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the device name of the mobility services engine that you want to edit.

Step 3 From the left sidebar menu, choose **Systems > Accounts > Users**.

Step 4 Select the check box(es) of the user(s) that you want to delete.

Step 5 From the Select a command drop-down list, choose **Delete User**.

Step 6 Click **Go**.

Step 7 Click **OK** to confirm that you want to delete the selected users.

Editing User Properties

To change user properties, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the device name of the mobility services engine that you want to edit.

Step 3 From the left sidebar menu, choose **Systems > Accounts > Users**.

Step 4 Click the username of the user that you want to edit.

Step 5 Make the required changes to the Password, Group Name, and Permission text boxes.

Step 6 Click **Save** to apply your change.

Adding User Groups

To add a user group to a mobility services engine, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the device name of the mobility services engine that you want to edit.

Step 3 From the left sidebar menu, choose **Systems > Accounts > Groups**.

Step 4 From the Select a command drop-down list, choose **Add Group**.

Step 5 Click **Go**.

Step 6 Enter the name of the group in the Group Name text box.

Step 7 Choose a permission level from the Permission drop-down list.

There are three permissions levels to choose from:

- **Read Access**
- **Write Access**
- **Full Access** (required for NCS to access mobility services engines)

Step 8 Click **Save** to add the new group to the mobility services engine.

Caution Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with read access permission, that user cannot configure mobility services engine settings.

Deleting User Groups

To delete user groups from a mobility services engine, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the device name of the mobility services engine that you want to edit.

Step 3 From the left sidebar menu, choose **Systems > Accounts > Groups**.

Step 4 Select the check box(es) of the group(s) that you want to delete.

Step 5 From the Select a command drop-down list, choose **Delete Group**.

Step 6 Click **Go**.

Step 7 Click **OK** to confirm that you want to delete the selected users.

Editing Group User Permissions

To change user group permissions, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the device name of the mobility services engine that you want to edit.

Step 3 From the left sidebar menu, choose **Systems > Accounts > Groups**.

Step 4 Click the group name of the group that you want to edit.

Step 5 Choose a permission level from the Permission drop-down list.

Step 6 Click **Save** to apply your change.

Caution Group permissions override individual user permissions. For example, if you give a user permission for full access and add that user to a group with read access, that user is unable to configure mobility services engine settings.

Monitoring Status Information for a Mobility Services Engine

The System > Status page enables you to monitor server events, NCS alarms and events, and NMSP connection status for the mobility services engine.

This section provides additional information and contains the following topics:

- Viewing Server Events for a Mobility Services Engine, page 11-39
- Viewing NCS Alarms for a Mobility Services Engine, page 11-40
- Viewing NCS Events for a Mobility Services Engine, page 11-40
- Viewing NMSP Connection Status for a Mobility Services Engine, page 11-41

Viewing Server Events for a Mobility Services Engine

To view a list of server events, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the applicable mobility services engine.

Step 3 From the left sidebar menu, choose **System > Status > Server Events**.

The Status > Server Events page provides the following information:

- Timestamp—Time of the server event.
- Severity—Severity of the server event.
- Event—Detailed description of the event.
- Facility—The facility in which the event took place.

Viewing Audit Logs from a Mobility Services Engine

You can view the audit logs for User-triggered operations using the Audit Logs option available in a Mobility Services Engine. To view the audit logs, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the applicable mobility services engine.

Step 3 From the left sidebar menu, choose **System > Status > Audit Logs**.

The **Status > Audit Logs** page provides the following information:

- Username—The Username which has triggered the audit log.
- Operation—The operation that has been performed by the User.
- Operation Status—The status of the operation and it can be SUCCESSFUL or FAILED.
- Invocation Time—The date and time at which the audit log was recorded for the specified operation.

Viewing NCS Alarms for a Mobility Services Engine

To view a list of NCS alarms, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the applicable mobility service.

Step 3 From the left sidebar menu, choose **System > Status > NCS Alarms**. See the "Monitoring Alarms" section on page 5-131 for more information.

Viewing NCS Events for a Mobility Services Engine

To view a list of NCS events, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the applicable mobility service.

Step 3 From the left sidebar menu, choose **System > Status > NCS Events**. See the "Monitoring Events" section on page 5-149 for more information.

Viewing NMSP Connection Status for a Mobility Services Engine

The NMSP Connection Status page allows you to verify the NMSP connection between the mobility services engine and the Cisco controller to which the mobility services engine is assigned.

Note Network Mobility Services Protocol (NMSP) is the protocol that manages communication between the mobility service and the controller.

To verify the NMSP connection between the controller and the mobility services engine, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the applicable mobility service.

Step 3 From the left sidebar menu, choose **System > Status > NMSP Connection Status**.

The NMSP Connection Status page shows the following information:

- Summary—The Summary section shows each device type, the total number of connections, and the number of inactive connections.
- NMSP Connection Status—This group box shows the following:
  - IP address—Click the device IP address to view NMSP connection status details for this device. See the "Viewing NMSP Connection Status Details" section on page 11-41 for additional information.
  - Target Type—Indicates the device to which the NMSP connection is intended.
  - Version—Indicates the current software version for the device.
  - NMSP Status—Indicates whether the connection is active or inactive.
  - Echo Request Count—Indicates the number of echo requests that were sent.
  - Echo Response Count—Indicates the number of echo responses that were received.
  - Last Message Received—Indicates the date and time of the most recent message received.

Step 4 Verify that the NMSP Status is ACTIVE.

- If active, you can view details on wired switches, controllers, and wired clients.
- If not active, resynchronize the NCS device and the mobility services engine.

Note You can launch an NMSP troubleshooting tool for an inactive connection.

Viewing NMSP Connection Status Details

To view NMSP Connection Status details, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the applicable mobility service.

Step 3 From the left sidebar menu, choose **System > Status > NMSP Connection Status**.

Step 4 Click the device IP address to open the NMSP Connection Status Details page. The Details page shows the following information:

- Summary
  - IP Address
  - Version—The current software version for the device.
  - Target Type—The device to which the NMSP connection is intended.
  - NMSP Status—Indicates whether the connection is active or inactive.
  - Echo Request Count—The number of echo requests that were sent.
  - Echo Response Count—The number of echo responses that were received.
  - Last Activity Time—The date and time of the most recent message activity between the device and the mobility services engine.
  - Last Echo Request Message Received At—The date and time the last echo request was received.
  - Last Echo Response Message Received At—The date and time the last echo response was received.
  - Model—The device model.
  - MAC Address—The MAC address of the device, if applicable.
  - Capable NMSP Services—Indicates the NMSP-capable services for this device such as ATTACHMENT or LOCATION.
- Subscribed Services—Indicates subservices for each subscribed NMSP service. For example, MOBILE_STATION_ATTACHMENT is a subservice of ATTACHMENT.
- Messages
  - Message Type—Message types might include: ATTACHMENT_NOTIFICATION, ATTACHMENT_REQUEST, ATTACHMENT_RESPONSE, CAPABILITY_NOTIFICATION, ECHO_REQUEST, ECHO_RESPONSE, LOCATION_NOTIFICATION, LOCATION_REQUEST, SERVICE_SUBSCRIBE_REQUEST, SERVICE_SUBSCRIBE_RESPONSE.
  - In/Out—Indicates whether the message was an incoming or outgoing message.
  - Count—Indicates the number of incoming or outgoing messages.
  - Last Activity Time—The date and time of the most recent activity or message.
  - Bytes—Size of the message in Bytes.

Managing Maintenance for Mobility Services

This section contains the following topics:

- Restoring Mobility Services Engine Historical Data, page 11-44
- Downloading Software to a Mobility Services Engine Using NCS, page 11-44

Viewing or Editing Mobility Services Backup Parameters

To view or edit mobility service backup parameters, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility service whose properties you want to edit.

Step 3 From the left sidebar menu, choose **Maintenance > Backup**.

- Backups located at—Indicates the location of the backup file.
- Enter a name for the Backup—Enter or edit the name of the backup file.
- Timeout (in secs)—Indicates the length of time (in seconds) before attempts to back up files times out.

Backing Up Mobility Services Engine Historical Data

NCS contains functionality for backing up mobility services engine data.

To back up mobility services engine data, follow these steps:

Step 1 In NCS, click **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to back up.

Step 3 From the left sidebar menu, choose **Maintenance > Backup**.

Step 4 Enter the name of the backup.

Step 5 Enter the time in seconds after which the backup times out.

Step 6 Click **Submit** to back up the historical data to the hard drive of the server running NCS.

Status of the backup can be seen on the page while the backup is in process. Three items are displayed on the page during the backup process: (1) Last Status field provides messages noting the status of the backup; (2) Progress field shows what percentage of the backup is complete; and (3) Started at field shows when the backup began noting date and time.

Note You can run the backup process in the background while working on other mobility services engine operations in another NCS page.

Note Backups are stored in the FTP directory that you specify during the NCS installation. However, in the NCS installation, the FTP directory is not specified. It might be necessary to provide the full path of the FTP root.

Restoring Mobility Services Engine Historical Data

To restore a file back into the mobility service, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility service whose properties you want to edit.

Step 3 From the left sidebar menu, choose **Maintenance > Restore**.

Step 4 Choose the file to restore from the drop-down list.

Step 5 Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the mobility services engine.

This option is applicable for network designs, wired switches, controllers and event definitions. The existing location history data is retained, however you must use manual service assignments to perform any future location calculations.

Step 6 Click **Submit** to start the restoration process.

Step 7 Click **OK** to confirm that you want to restore the data from the NCS server hard drive.

When the restoration is complete, NCS shows a message to that effect.

Note You can run the restore process in the background while working on other mobility services engine operations in another NCS page.

Downloading Software to a Mobility Services Engine Using NCS

To download software to a mobility services engine using NCS, follow these steps:

Step 1 Verify that you can ping the location appliance from NCS or an external FTP server, whichever you are going to use for the application code download.

Step 2 Choose **Services > Mobility Services**.

Step 3 Click the name of the mobility services engine to which you want to download software.

Step 4 On the left sidebar menu, choose **Maintenance**.

Step 5 Click *Download Software*.

To download software, do one of the following:

- To download software listed in the NCS directory, select the *Select from uploaded images to transfer into the Server* check box. Then, choose a binary image from the drop-down list.

  NCS downloads the binary images listed in the drop-down list into the FTP server directory you specified during the NCS installation.

  In NCS installation, FTP directory is not specified. It might be necessary to give the full path of the FTP root.

- To use downloaded software available locally or over the network, select the **Browse a new software image to transfer into the Server** check box and click **Browse**. Locate the file and click **Open**.

Step 6 Enter the time, in seconds (between 1 and 1800), after which the software download times out.

Step 7 Click **Download** to send the software to the /opt/installers directory on the mobility services engine.

Managing Cisco Adaptive wIPS Service Parameters

The wIPS Service page allows you to view or manage wIPS service administrative settings.

Note Cisco Adaptive wIPS functionality is not supported for non-root partition users.

Managing wIPS Service Administration Settings

To view or manage wIPS service administration settings, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Choose the device name of the applicable mobility services engine.

Step 3 From the left sidebar menu, choose **wIPS Service**.

Step 4 View or edit the following parameters:

- Log level—Choose the applicable log level from the drop-down list. Log levels include debug, error, important event, major debug, none, and warning.
- Forensic size limit (GB)—Enter the maximum allowable size of forensic files.
- Alarm ageout (hours)—Enter the age limit, in hours, for each alarm.
- Device ageout (days)—Enter the age limit, in days, for the device to send alarms.

Step 5 Click **Save** to confirm the changes or **Cancel** to close the page with no changes applied.

Managing Context-Aware Service Software Parameters

Context-Aware Service (CAS) software allows a mobility services engine to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location, temperature and asset availability about a client or tag (Cisco CX version or later) from Cisco access points.

CAS relies on two engines for processing the contextual information it receives. The *Context-Aware Engine for Clients* processes data received from Wi-Fi clients and the *Context-Aware Engine for Tags* processes data received from Wi-Fi tags; these engines can be deployed together or separately depending on the business need.

Note Mobility services engines do not track or map non-Cisco CX tags.

Note CAS was previously referred to as Cisco location-based services.

You can modify Context-Aware Service Software properties as to the type and number of clients or tags that are tracked and whether or not locations are calculated for those clients or tags.

You can also modify parameters that affect the location calculation of clients and tags such as Received Signal Strength Indicator (RSSI) measurements.

Viewing Contextual Information

Before you can use NCS to view contextual information, initial configuration for the mobility services engine is required using a command-line interface (CLI) console session. See the *Cisco 3350 Mobility Services Engine Getting Started Guide* and the *Cisco 3100 Mobility Services Engine Getting Started Guide* at the following URL: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

After its installation and initial configuration are complete, the mobility services engine can communicate with multiple Cisco wireless LAN controllers to collect operator-defined contextual information. You can then use the associated NCS to communicate with each mobility services engine to transfer and display selected data.

You can configure the mobility services engine to collect data for clients, rogue access points, rogue clients, mobile stations, interferers, and active RFID asset tags.

Licensing for Clients and Tags

You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points.

- Licenses for tags and clients are offered separately.
- The clients license also contains tracking of rogue clients and rogue access points, and interferers (if enabled).
- Licenses for tags and clients are offered in a variety of quantities, ranging from 1,000 to 12,000 units.

  The AeroScout Context-Aware Engine for Tags support 100 permanent tag licenses; Context-Aware Services consists of permanent tag licenses.

Note See the *Release Notes for Cisco 3300 Series Mobility Services Engine for Software Release 6.0* at the following URL: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html for more information on tags and client licenses.

For additional information on Context-Aware parameters, select one of the following topics:

- Context-Aware Service General Parameters, page 11-46
- Context-Aware Service Administration Parameters, page 11-47
- Context-Aware Service Advanced Parameters, page 11-64

Context-Aware Service General Parameters

To access the Context Aware Service > General page, choose **Services > Mobility Services > General** from the left sidebar menu. This page provides the following information:

- Number of tracked clients
- Number of traced tags
- Number of tracked rogues

- Number of tracked interferers
- Number of tracked wired clients
- Limit for total elements tracked
- Limit for number of tracked tags
- Interactive graph of the mobility services engine client and tag count

Context-Aware Service Administration Parameters

This section contains the following topics:

Modifying Tracking Parameters for Mobility Services

The mobility services engine can track up to18,000 clients or up to18,000 tags (with the proper license purchase). Updates on the locations of elements being tracked are provided to the mobility services engine from the Cisco wireless LAN controller.

Only those elements designated for tracking by the controller are viewable in NCS maps, queries, and reports. No events and alarms are collected for non-tracked elements and none are used in calculating the 18,000 element limit for clients or tags.

You can modify the following tracking parameters using NCS:

- Enable and disable element locations (client stations, active asset tags, interferers, wired clients, rogue clients, and rogue access points) you actively track.
  - Wired client location tracking enables servers in a data center to more easily find wired clients in the network. Servers are associated with wired switch ports in the network.
- Set limits on how many of specific elements you want to track.

  For example, given a client license of 12,000 trackable units, you can set a limit to track only 8,000 client stations (leaving 4,000 units available to track rogue clients and rogue access points). Once the tracking limit is met for a given element, the number of elements not being tracked is summarized in the Tracking Parameters page.
- Disable tracking and reporting of ad hoc rogue clients and access points.

To configure tracking parameters for a mobility services engine, follow these steps:

Step 1 Choose **Services > Mobility Services** to open the Mobility Services page.

Step 2 Click the name of the mobility services engine whose properties you want to edit. The General Properties page opens.

Step 3 In the Context-Aware Software menu located on the left sidebar menu, choose **Tracking Parameters** from the Administration subheading to display the configuration options.

Step 4 Modify the following tracking parameters as appropriate (see Table 11-5).

Table 11-5 Tracking Parameters

Field	Configuration Options
Tracking Parameters	
Wired Clients	1. Select the **Enable** check box to enable tracking of client stations by the mobility services engine. In 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers. The wired client limiting is supported from mobility services engine 7.0 and NCS 1.0. In other words, you can limit wired clients to a fixed number, say 500. This limit is set to ensure that the licenses are not taken up completely by wired clients and some licenses are available for other devices. **Caution** When upgrading the mobility services engine from 6.0 to 7.0, if any limits have been set on wireless clients or rogues, they reset because of the wired client limit change in 7.0. **Note** Active Value (Display only): Indicates the number of wired client stations currently being tracked. **Note** Not Tracked (Display only): Indicates the number of wired client stations beyond the limit.
Wireless Clients	1. Select the **Enable** check box to enable tracking of client stations by the mobility services engine. 2. Select the **Enable Limiting** check box to set a limit on the number of client stations to track. 3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 18,000 which is the maximum number of clients that can be tracked by a mobility services engine. **Note** The actual number of tracked clients is determined by the license purchased. **Note** Active Value (Display only): Indicates the number of client stations currently being tracked. **Note** Not Tracked (Display only): Indicates the number of client stations beyond the limit.

Table 11-5 Tracking Parameters (continued)

Field	Configuration Options
Rogue Access Points	1. Select the **Enable** check box to enable tracking of rogue clients and asset points by the mobility services engine. 2. Select the **Enable Limiting** check box to set a limit on the number of rogue clients and asset tags stations to track. 3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to18,000 which is the maximum number of rogue clients and access points that can be tracked by a mobility services engine. **Note** The actual number of tracked rogues (clients and access points) is driven by the client license purchased. The user must consider the number of clients that are being tracked in determining the available quantity to allocate to track rogue clients and access points because clients and rogue clients and access points are addressed by the same license. **Note** Active Value (Display only): Indicates the number of rogue clients and access points currently being tracked. **Note** Not Tracked (Display only): Indicates the number of rogue clients and access points beyond the limit.
Exclude Ad-Hoc Rogues	Select the check box to turn off the tracking and reporting of ad hoc rogues in the network. As a result, ad hoc rogues are not displayed on NCS maps or its events and alarms reported.
Rogue Clients	1. Select the **Enable** check box to enable tracking of rogue clients by the mobility services engine. 2. Select the **Enable Limiting** check box to set a limit on the number of rogue clients to track. 3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to18,000 which is the maximum number of rogue clients that can be tracked by a mobility services engine. **Note** The actual number of tracked rogues (clients and access points) is driven by the client license purchased. The user must consider the number of clients that are being tracked in determining the available quantity to allocate to track rogue clients and access points because clients and rogue clients and access points are addressed by the same license. **Note** Active Value (Display only): Indicates the number of rogue clients being tracked. **Note** Not Tracked (Display only): Indicates the number of rogue clients beyond the limit.

Table 11-5 Tracking Parameters (continued)

Field	Configuration Options
Interferers	1. Select the **Enable** check box to enable tracking of the interferers by the mobility services engine. In 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers. **Note** Active Value (Display only): Indicates the number of interferers currently being tracked. **Note** Not Tracked (Display only): Indicates the number of interferers beyond the limit.
Asset Tracking Elements	
Active RFID Tags	1. Select the **Enable** check box to enable tracking of active RFID tags by the mobility services engine. **Note** The actual number of tracked active RFID tags is determined by the license purchased. **Note** Active Value (Display only): Indicates the number of active RFID tags currently being tracked. It also depends on the tag engine chosen. **Note** Not Tracked (Display only): Indicates the number of active RFID tags beyond the limit.
SNMP Parameters Not applicable to mobility services 7.0.105.0 and later.	
SNMP Retry Count	Enter the number of times to retry a polling cycle the default value is 3. Allowed values are from 1 to 99999. (Configurable in controller release 4.1 and earlier only.)
SNMP Timeout	Enter the number of seconds before a polling cycle times out, the default value is 5. Allowed values are from 1 to 99999. (Configurable in controller release 4.1 and earlier only.)
SNMP Polling Interval	
Client Stations	Select the **Enable** check box to enable client station polling and enter the polling interval in seconds. Default value is 300. Allowed values are from 1 to 99999. (Configurable in controller release 4.1 and earlier only.)
Active RFID Tags	Select the **Enable** check box to enable active RFID tag polling and enter the polling interval in seconds. Allowed values are from 1 to 99999. **Note** Before the mobility service can collect asset tag data from controllers, you must enable the detection of active RFID tags using the **config rfid status enable** CLI command on the controllers.
Rogue Clients and Access Points	Select the **Enable** check box to enable rogue access point polling and enter the polling interval in seconds. Default value is 600. Allowed values are from 1 to 99999.(Configurable in controller release 4.1 and earlier only.)
Statistics	Select the **Enable** check box to enable statistics polling for the mobility service, and enter the polling interval in seconds. Default value is 900. Allowed values are from 1 to 99999.(Configurable in controller release 4.1 and earlier only.)

Step 5 Click **Save** to store the new settings in the mobility services engine database.

Filtering Parameters for Mobility Services

In NCS, you can limit the number of asset tags, wired clients, rogue clients, interferers and access points whose location is tracked by filtering on the following:

- MAC addresses

  Specific MAC addresses can be entered and labeled as allowed or disallowed from location tracking. You can import a file with the MAC addresses that are to be allowed or disallowed, or you can enter them individually in the NCS GUI page.

  The format for entering MAC addresses is xx:xx:xx:xx:xx:xx. If a file of MAC addresses is imported, the file must follow a specific format as follows:

  - Each MAC address should be listed on a single line.
  - Allowed MAC addresses must be listed first and preceded by an "[Allowed]" line item. Disallowed MAC addresses must be preceded by "[Disallowed]."
  - Wildcard listings can be used to represent a range of MAC addresses. For example, the first entry "00:11:22:33:*" in the Allowed listing that follows is a wildcard.

Note Allowed MAC address formats are viewable in the Filtering Parameters configuration page. See Table 11-6 for details.

EXAMPLE file listing:

```
[Allowed]
00:11:22:33:*
22:cd:34:ae:56:45
02:23:23:34:*
[Disallowed]
00:10:*
ae:bc:de:ea:45:23
```

- Probing clients

  Probing clients are clients that are associated to another controller but whose probing activity causes them to be seen by another controller and be counted as an element by the "probed" controller as well as its primary controller.

Modifying Filtering Parameters

To configure filtering parameters for a mobility services engine, follow these steps:

Step 1 Choose **Services > Mobility Services**. The Mobility Services page appears.

Step 2 Click the name of the mobility services engine whose properties you want to edit. The General Properties page appears.

Step 3 From the Context-Aware Software menu, choose **Filtering Parameters** from the Administration subheading to display the configuration options.

Step 4 Modify the following filtering parameters as appropriate (see Table 11-6).

Table 11-6 Filtering Parameters

Field	Configuration Options
Exclude Probing Clients	Select the check box to prevent location calculation of probing clients.
Enable Location MAC Filtering	1. Select the check box to enable MAC filtering of specific elements by their MAC address. 2. To import a file of MAC addresses (Upload a file for Location MAC Filtering field), browse for the filename and click **Save** to load the file. The imported list of MAC addresses auto-populates the Allowed List and Disallowed List based on their designation in the file. **Note** To view allowed MAC address formats, click the red question mark next to the Upload a file for Location MAC Filtering field. 3. To add an individual MAC address, enter the MAC addresses (format is xx:xx:xx:xx:xx:xx) and click either **Allow** or **Disallow**. The address appears in the appropriate column. **Note** To move an address between the Allow and Disallow columns, highlight the MAC address entry and click the button under the appropriate column. **Note** To move multiple addresses, click the first MAC address and press **Ctrl** to highlight additional MAC addresses. Click **Allow** or **Disallow** based on its desired destination. **Note** If a MAC address is not listed in the Allow or Disallow column, by default, it appears in the Blocked MACs column. If you click the **Unblock** button, the MAC address automatically moves to the Allow column. You can move it to the Disallow column by selecting the Disallow button under the Allow column.

Step 5 Click **Save** to store the new settings in the mobility services engine database.

Modifying History Parameters for Mobility Services

You can use NCS to specify how long to store (archive) histories on client stations, rogue clients, and asset tags. These histories are received from those controllers that are associated with the mobility service.

You can also program the mobility service to periodically remove (prune) duplicate data from its historical files to reduce the amount of data stored on its hard drive.

To configure mobility service history settings, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility service whose properties you want to edit.

Step 3 From the left sidebar menu, choose **Context Aware Service > History Parameters**.

Step 4 Modify the following history parameters as appropriate (see Table 11-7).

Table 11-7 History Parameters

:

Field	Description
Archive for	Enter the number of days for the location appliance to retain a history of each enabled category. The default value is 30. Allowed values are from 1 to 99999.
Prune data starting at	Enter the number of hours and minutes at which the location appliance starts data pruning (between 0 and 23 hours, and between 1 and 59 minutes). Enter the interval in minutes after which data pruning starts again (between 0, which means never, and 99900000). The default start time is 23 hours and 50 minutes, and the default interval is 1440 minutes.
Enable History Logging of Location Transitions for	To enable history logging of Location transitions, choose one or more of the following: • Client Stations • Wired Stations • Asset Tags • Rogue Clients • Rogue Access Points • Interferers **Note** Before the mobility service can collect asset tag data from controllers, you must enable the detection of RFID tags using the **config rfid status enable** CLI command.

Step 5 Click **Save** to store your selections in the location appliance database.

Enabling Location Presence for Mobility Services

You can enable location presence on the mobility services engine to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by wireless and wired clients on a demand basis for use by location-based services and applications.

You can also import advanced location information such as the MAC address of a wired client and the wired switch slot and port to which the wired client is attached.

Location Presence can be configured when a new Campus, Building, Floor or Outdoor Area is being added or configured at a later date.

Once enabled, the mobility services engine is capable of providing any requesting Cisco CX v5 client its location.

Note Before enabling this feature, synchronize the mobility services engine.

To enable and configure location presence on a mobility services engine, follow these steps:

Step 1 Choose **Services > Mobility Services >** *Device Name*. Select the mobility services engine to which the campus or building or floor is assigned.

Step 2 From the left sidebar menu, choose **Context Aware Services > Administration > Presence Parameters**.

Step 3 Select the Service Type **On Demand** check box to enable location presence for Cisco CX clients v5.

Step 4 Select one of the following Location Resolution options:

a. When Building is selected, the mobility services engine can provide any requesting client, its location by building.

- For example, if a client requests its location and the client is located in Building A, the mobility services engine returns the client address as Building A.

b. When AP is selected, the mobility services engine can provide any requesting client, its location by its associated access point. The MAC address of the access point appears.

- For example, if a client requests its location and the client is associated with an access point with a MAC address of 3034:00hh:0adg, the mobility services engine returns the client address of 3034:00hh:0adg.

c. When X,Y is selected, the mobility services engine can provide any requesting client, its location by its X and Y coordinates.

- For example, if a client requests its location and the client is located at (50, 200) the mobility services engine returns the client address of 50, 200.

Step 5 Select any or all of the location formats:

a. Select the **Cisco** check box to provide location by campus, building and floor and X and Y coordinates. Default setting.

b. Select the **Civic** check box to provide the name and address (street, city, state, postal code, country) of a campus, building, floor, or outdoor area.

Note See the "Importing Civic Information for Mobility Services" section on page 11-56 for more information on importing a file with multiple Civic listings.

c. Select the **GEO** check box to provide the longitude and latitude coordinates.

Step 6 By default, the Text check box for Location Response Encoding is selected. It indicates the format of the information when received by the client. There is no need to change this setting.

Step 7 Select the **Retransmission Rule Enable** check box to allow the receiving client to retransmit the received information to another party.

Step 8 Enter a Retention Expiration value in minutes. This determines how long the received information is stored by the client before it is overwritten. The default value is 24 hours (1440 minutes).

Step 9 Click **Save**.

Importing Asset Information for Mobility Services

To import asset, chokepoint, and TDOA receiver information for the mobility services engine using NCS, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine for which you want to import information.

Step 3 Choose **Context Aware Service > Administration > Import Asset Information**.

Step 4 Enter the name of the text file or browse for the filename.

Specify information in the imported file in the following formats:

- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

Step 5 When the import filename is located in the Browse text box, click **Import**.

Exporting Asset Information for Mobility Services

To export asset, chokepoint, and TDOA receiver information from the mobility services engine to a file using NCS, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine from which you want the export information.

Step 3 Choose **Context Aware Service > Administration > Export Asset Information**.

Information in the exported file is in the following formats:

- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

Step 4 Click **Export**.

Click **Open** (display to screen), **Save** (to external PC or server), or **Cancel** (to cancel the request).

Note If you select **Save**, you are asked to select the asset file destination and name. The file is named assets.out by default. Click **Close** in the dialog box when the download is complete.

Importing Civic Information for Mobility Services

To import civic information for the mobility services engine using NCS, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine for which you want to import asset information.

Step 3 From the left sidebar menu, choose **Context Aware Software**.

Step 4 From the Administration left sidebar menu, choose **Import Civic Information**.

Step 5 Enter the name of the text file or browse for the filename.

Information in the imported file should be one of the following formats:

Switch IP Address, Slot Number, Port Number, Extended Parent Civic Address, X, Y, Floor ID, Building ID, Network Design ID, ELIN:"ELIN", PIDF-Lo-Tag:"Civic Address Element Value"

Note Each entry must appear on a separate line.

Step 6 Click **Import**.

Context-Aware Service Wired Parameters

This section describes the Context Aware Service > Wired drop-down list parameters and contains the following topics:

Monitoring Wired Switches

You can review details on the wired switch (IP address, MAC address, serial number, software version, and ELIN), its port, its wired clients (count and status), and its civic information.

Wired switch data is downloaded to the mobility services engine through NCS when the Ethernet switch and the mobility services engine are synchronized (Services > Synchronize Services > Switches). Communication between a location-capable switch and the mobility services engine is over NMSP. NCS and the mobility services engine communicate over XML.

To view details on wired switches, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 In the Mobility Services page, click the device name link of the appropriate wired location switch.

Step 3 Choose **Context Aware Service > Wired > Wired Switches**. A summary of wired switches that are synchronized with the mobility services engine appears.

Step 4 See the "Wired Switch Details" section on page 11-57 for more information on the switch, its port, its wired clients (count and status), and its civic information click the IP address link.

Wired Switch Details

To view wired switch details, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 In the Mobility Services page, click the device name link of the appropriate mobility services engine.

Step 3 Choose **Context Aware Service > Wired > Wired Switches**. A summary of wired switches that are synchronized with the mobility services engine appears.

Step 4 Click the IP address link for the applicable wired switch. The Wired Switch Details page opens.

The Wired Switch Details page has four tabs: Switch Information, Switch Ports, Civic, and Advanced.

Note You can export civic information from the switch by choosing that option from the Select a command drop-down list. This option is available in all four dashlets of the Wired Switches page.

The Wired Switch Details tabs shows the following information:

- Switch Information—Displays a total count summary of wired clients connected to the switch along with the state of the client (connected, disconnected, and unknown).
  - Connected clients—Clients that are connected to the wired switch.
  - Disconnected clients—Clients that are disconnected from the wired switch.
  - Unknown clients—Clients are marked as unknown when the NMSP connection to the wired switch is lost.

  Note You can view detailed wired client information by clicking in one of the client count links (total clients, connected, disconnected, and unknown). See the "Monitoring Wired Clients" section on page 11-58 section for more information.

- Switch Ports—Displays a detailed list of the ports on the switch.

  Note You can change the listing order (ascending, descending) of port IP addresses, slot numbers, module number, port type, and port number by clicking in the respective column heading.

- Civic—Displays a detailed list of the civic information for the wired switch.

- Advanced—Displays a detailed list of the additional civic information for the wired switch.

Monitoring Wired Clients

You can view details on a wired client (MAC address, IP address, username, serial number, UDI, model no., software version, VLAN ID, and VLAN ID), port association, and its civic information.

Wired client data is downloaded to the mobility services engine through NCS when the switch and the mobility services engine are synchronized (Services > Synchronize Services > Switches).

NCS and the mobility services engine communicate over XML.

You can view the details of the wired client on either the wired switches page (Context Aware Service > Wired > Wired Switches) or wired clients page (Context Aware Service > Wired > Wired Clients).

- If you know the IP address, MAC address, VLAN ID, serial number, or username, you can use the search field on the wired clients page.
- If you want to examine wired clients as they relates to a specific switch, you can view that information on the wired switches page. See the "Monitoring Wired Switches" section on page 11-56 section for more information.

To view details on a wired client, follow these steps:

Step 1 Choose **Services > Mobility Services**. The Mobility Services page opens.

Step 2 Click the device name link of the appropriate wired location switch.

Step 3 Choose **Context Aware Service > Wired > Wired Clients**.

In the Wired Clients summary page, clients are grouped by their switch.

A client status is noted as connected, disconnected, or unknown:

- Connected clients—Clients that are active and connected to a wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the NMSP connection to the wired switch is lost. See the "Viewing NMSP Connection Status for a Mobility Services Engine" section on page 11-41 for more information about NMSP connections.

If you know the MAC address of the wired client, you can click that link to reach the detail page of the client or use the search field. See the "Wired Client Details" section on page 11-58 for more information on wired client details.

- You can also search for a wired client by its IP address, username, or VLAN ID.

If you click the IP address of the switch, you are forwarded to the detail page of the switch. See the "Monitoring Wired Switches" section on page 11-56 section for more information.

Step 4 Click the MAC Address for the applicable client to view wired client details. See the "Wired Client Details" section on page 11-58 for more information on wired client details.

Wired Client Details

To view wired client details, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 In the Mobility Services page, click the device name link of the appropriate mobility services engine.

Step 3 Choose **Context Aware Service > Wired > Wired Clients**. A summary of wired clients that are synchronized with the mobility services engine appears.

Step 4 Click the MAC address link for the applicable wired client. The Wired Client Details page opens.

The Wired Client Details page has four tabs: Device Information, Port Association, Civic Address, and Advanced.

The Wired Switch Details tabs show the following information:

- Device Information—Display MAC and IP address, username, serial and model number, UDI, software version, VLAN ID, and VLAN name.
- Port Association—Displays the physical location of the switch port/slot/module on which the wired client terminates, the client status (connected, disconnected, unknown), and the switch IP address.
- Civic Address—Displays any civic address information.
- Advanced—Displays extended physical address details for the wired clients, if applicable.

Note A client takes on the civic address and advanced location information that is configured for the port on which the client terminates. If no civic and advanced information is defined for the its port (port/slot/module) then no location data is displayed.

Monitoring Interferers

The Monitor > Interferers page allows you to monitor interference devices detected by the CleanAir enabled access points.

This section provides information on the interferers detected by the CleanAir enabled access points. By default, the Monitor > Interferers > AP Detected Interferers, page 11-59 page is displayed.

This section contains the following topics:

Monitor > Interferers > AP Detected Interferers

Choose **Monitor > Interferers** to view all the interfering devices detected by the CleanAir enabled access points on your wireless network. This page enables you to view a summary of the interfering devices including the following default information:

- Interferer ID—A unique identifier for the interferer. Click this link to know more about the interferer.
- Type—Indicates the category of the interferer. Click to read more about the type of device. The dialog box appears displaying more details. The categories include the following:
  - Bluetooth link—A Bluetooth link (802.11b/g/n only)
  - Microwave Owen—A microwave oven (802.11b/g/n only)

  - 802.11 FH—An 802.11 frequency-hopping device (802.11b/g/n only)
  - Bluetooth Discovery—A Bluetooth discovery (802.11b/g/n only)
  - TDD Transmitter—A time division duplex (TDD) transmitter
  - Jammer—A jamming device
  - Continuous Transmitter—A continuous transmitter
  - DECT-like Phone—A digital enhanced cordless communication (DECT)-compatible phone
  - Video—A video camera
  - 802.15.4—An 802.15.4 device (802.11b/g/n only)
  - WiFi Inverted—A device using spectrally inverted Wi-Fi signals
  - WiFi Invalid—A device using non-standard Wi-Fi channels
  - SuperAG—An 802.11 SuperAG device
  - Canopy—A Motorola Canopy device
  - Radar—A radar device (802.11a/n only)
  - XBox—A Microsoft Xbox (802.11b/g/n only)
  - WiMAX Mobile—A WiMAX mobile device (802.11a/n only)
  - WiMAX Fixed—A WiMAX fixed device (802.11a/n only)
  - TDD Exalt
  - Motorola Canopy
- Status—Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir-enabled access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir-enabled access point or the CleanAir-enabled access point determined that the interferer is no longer reachable by NCS.
- Severity—Displays the severity ranking of the interfering device.
- Affected Band—Displays the band in which this device is interfering.
- Affected Channels—Displays the affected channels.
- Duty Cycle (%)—The duty cycle of interfering device in percentage.
- Discovered—Displays the time at which it was discovered.
- Last Updated—The last time the interference was detected.
- Floor—The location where the interfering device is present.

Note These devices appear only if the option to track Interferers is enabled in the Tracking Parameters page. This option is disabled by default. See the "Modifying Tracking Parameters for Mobility Services" section on page 11-47 for more information on tracking parameters.

Monitor > Interferers > AP Detected Interferers > Interferer Details

Choose **Monitor** > **Interferers** > *Interferer ID* to view this page. This page enables you to view the details of the interfering devices detected by the access points. This page provides the following details about the interfering device.

- Interferer Properties
  - Type—Displays the type of the interfering device detected by the AP.
- Status—The status of the interfering device. Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir enabled access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir enabled access point or the CleanAir enabled access point saw the interferer no longer reachable by NCS.
  - Severity—Displays the severity ranking of the interfering device.
  - Duty Cycle (%)—The duty cycle of interfering device in percentage.
  - Affected Band—Displays the band in which this device is interfering.
  - Affected Channels—Displays the affected channels.
  - Discovered—Displays the time at which it was discovered.
  - Last Updated—The last time the interference was detected.
- Location
  - Floor—The location where this interfering device was detected.
  - Last Located At—The last time where the interfering device was located.
  - On MSE—The Mobility Server Engine on which this interference device was located.
- Clustering Information
  - Clustered By—Displays the following:

    IP address of the controller if clustered by a controller.

    IP address of the mobility services engine if clustered by a mobility services engine.
  - Detecting APs—Displays the details of the access point that has detected the interfering device. The details include: Access Point Name (Mac), Severity, and Duty Cycle(%).

Note The detecting access point information is available only for active devices. And even for some active devices, this information might not be available. This is because these interferers are in the process of being marked inactive and in the next refresh of Monitor > Interferers page, these appear as inactive.

- Details—Displays a short description about the interfering type.

Select a command

The Select a command drop-down list provides access to the location history of the interfering device detected by the access point. See the "Monitor > Interferers > AP Detected Interferer Details > Interference Device ID > Location History" section on page 11-62 for more information.

Monitor > Interferers > AP Detected Interferer Details > Interference Device ID > Location History

Choose **Monitor > Interferers >** *Interference Device ID*, choose **Location History** from the Select a command drop-down list, and click **Go** to view this page.

- Interferer Information—Displays the basic information about the interfering device.
  - Data Collected At—The time stamp at which the data was collected.
  - Type—The type of the interfering device.
  - Severity—The severity index of the interfering device.
  - Duty Cycle—The duty cycle (in percentage) of the interfering device.
  - Affected Channels—A comma separated list of the channels affected.
- Interferer Location History—Displays the location history of the interfering devices.
  - Time Stamp
  - Floor
- Clustering Information
  - Clustered By
- Detecting APs
  - AP Name—The access point that detected the interfering device.
  - Severity—The severity index of the interfering device.
  - Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.
- Location
  - Location Calculated At—Displays the time stamp at which this information was generated.
  - Floor—Displays location information of the interfering device.
  - A graphical view of the location of the interfering device is displayed in a map. Click the **Enlarge** link to view an enlarged image.

Monitor > Interferers > Edit View

The Edit View page allows you to add, remove, or reorder columns in the AP Detected Interferers Summary page. It also allows you to search for Interferers. By default, only those interferers that are in Active state and with a severity greater than or equal to 5 are displayed in the AP Detected Interferers page. See the "Monitor > Interferers > Edit View > Edit Search" section on page 11-63 for more information on editing search criteria.

To edit the columns in the AP Detected Interferers page, follow these steps:

Step 1 Choose **Monitor > Interferers**. The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir-enabled access points.

Step 2 Click the **Edit View** link in the AP Detected Interferers page.

Step 3 To add an additional column to the access points table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the table.

Step 4 To remove a column from the access points table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. All items in the left column are not displayed in the table.

Step 5 Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.

Step 6 Click **Reset** to restore the default view.

Step 7 Click **Submit** to confirm the changes.

Monitor > Interferers > Edit View > Edit Search

You can search for interferers based on certain criteria. By default only those interferers that are in Active state and with severity greater than or equal to 5 are displayed in the AP Detected Interferers page. Use the Edit Search option to customize the interferer search.

To edit the search criteria, follow these steps:

Step 1 Choose **Monitor > Interferers**. The AP Detected Interferers page appears.

Step 2 Click **Edit Search** and select the appropriate criteria. This option allows you to specify the following search criteria:

- Search Category—For interferer search, the search category is Interferers.
- Detected By—From the drop-down list, choose **Access Points** or **Spectrum Experts**.
- Search By—From the list box, choose any one of the following options:
  - **All Interferers**
  - **Interferer ID**
  - **Interferer Type**
  - **Severity**
  - **Duty Cycle**
  - **Location**
- Severity greater than—Enter the severity level in the text box.
- Detected within the last—From the list box, choose any one of the following options:
  - **5 Minutes**
  - **15 Minutes**
  - **30 Minutes**
  - **1 Hour**
  - **3 Hours**
  - **6 Hours**
  - **12 Hours**
  - **24 Hours**
  - **All History**
- Interferer status—From the list, choose any of the following options:
  - **Active**
  - **Inactive**
  - **All**

- Restrict By Radio Band/Channels—Select this check box if you want to restrict certain radio frequencies or channels from the search. By default, this check box is unselected. On selection of this check box, a list appears with 2.4-GHz, 5-GHz and Individual Channel options. If you select Individual Channel, an Affected Channels text box appears. Specify the channel and select either the **Match All** or **Match Any** radio button.

Step 3 Select the number of items per page that you want to view in the search results.

Step 4 Select the **Save Search** check box if you want to save the search.

Step 5 After specifying the search criteria. Click **Go** to view the search results.

Context-Aware Service Advanced Parameters

This section contains the following topics:

Modifying Location Parameters for Mobility Services

You can use NCS to specify whether the mobility service retains its calculation times and how soon the mobility service deletes its collected Received Signal Strength Indicator (RSSI) measurement times. You can also apply varying smoothing rates to manage location movement of an element.

To configure location parameters, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility service whose properties you want to edit.

Step 3 From the left sidebar menu, choose **Context Aware Service > Location Parameters**.

Step 4 Modify the location parameters as appropriate (see Table 11-8).

Table 11-8 Location Parameters

Field	Description
General	
Enable Calculation Time	Select the check box to enable the calculation of the time required to compute location. **Caution** Enable only under Cisco TAC personnel guidance because enabling this field slows down overall location calculations.

Table 11-8 Location Parameters (continued)

Field	Description
Enable OW Location	Select the check box to enable Outer Wall (OW) calculation as part of location calculation. **Note** The OW Location parameter is ignored by the location server.
Relative discard RSSI time	Enter the number of minutes since the most recent RSSI sample after which RSSI measurement should be considered stale and discarded. Default value is 3. Allowed values range from 0 to 99999. A value of less than 3 is not recommended.
Absolute discard RSSI time	Enter the number of minutes after which RSSI measurement should be considered stale and discarded, regardless of the most recent sample. Default value is 60. Allowed values range from 0 to 99999. A value of less than 60 is not recommended.
RSSI Cutoff	Enter the RSSI cutoff value, in decibels (dBs) with respect to one (1) mW (dBm), preceding which the mobility service always use the access point measurement. Default value is -75. **Note** When 3 or more measurements are available preceding the RSSI cutoff value, the mobility service discards any weaker values and use the 3 (or more) strongest measurements for calculation; however, when only weak measurements following the RSSI cutoff value are available, those values are used for calculation. **Caution** Modify only under Cisco TAC personnel guidance. Modifying this value can reduce the accuracy of location calculation.
Enable Location Filtering	If enabled, the location filter is applied only for client location calculation. Enabling location filter allows previous location estimates to be used in estimating current location. This reduces location jitter for stationary clients and improve tracking for mobile clients.

Table 11-8 Location Parameters (continued)

Field	Description
Chokepoint Usage	Select the check box to enable the usage of chokepoint proximity to determine location. Applies to Cisco compatible Tags capable of reporting chokepoint proximity.
Use Chokepoints for Interfloor conflicts	Allows the use of chokepoints to determine the correct floor during Interfloor conflicts. Choose **Never**, **Always**, or **Floor Ambiguity**.
Chokepoint Out of Range Timeout	After a Cisco compatible Tag leaves a chokepoint proximity range, this is the timeout (in seconds) after which RSSI information is used again to determine location.
Absent Data Cleanup Interval	Enter the interval period (in minutes) for removing inactive elements from the database.
Use Default Heatmaps for Non Cisco Antennas	Select this check box to enable the usage of default heatmaps for non-Cisco antennas during the Location Calculation. This option is disabled by default.
Movement Detection	
Individual RSSI change threshold	This field specifies the Individual RSSI movement recalculation trigger threshold. Enter a threshold value between 0-127 dBm. Donot modify without Cisco TAC guidance.
Aggregated RSSI change threshold	This field specifies the Aggregated RSSI movement recalculation trigger threshold. Enter a threshold value between 0-127 dBm. It should not be modified without Cisco TAC guidance.
Many new RSSI change percentage threshold	This field specifies Many new RSSI movement recalculation trigger threshold in percentage. It should not be modified without Cisco TAC guidance.
Many missing RSSI percentage threshold	This field specifies Many missing RSSI movement recalculation trigger threshold in percentage. It should not be modified without Cisco TAC guidance.

Step 5 Click **Save** to store your selections in the NCS and mobility service databases.

Modifying Notification Parameters for Mobility Services

You can use NCS to configure mobility services engine event notification parameters that define such items as how often the notifications are generated or resent by the mobility services engine.

Note Modify notification parameters only if you expect the mobility services engine to send a large number of notifications or if notifications are not being received.

You can also enable forwarding of northbound notifications for tags to be sent to third-party applications.

The format of northbound notifications sent by the mobility services engine is available on the Cisco developers support portal at the following URL:

http://www.cisco.com/en/US/products/svcs/ps3034/ps5408/ps5418/serv_home.html

To configure notification parameters, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine you want to configure.

Step 3 From the Context Aware Software left sidebar menu, choose **Notification Parameters** from the Advanced sub-heading to display the configuration options.

Step 4 Select the **Enable Northbound Notifications** check box to enable the function.

Step 5 Select the **Notification Contents** check box to send notifications to third-party applications (northbound).

Step 6 Select one or more of the following Notification content options:

- Chokepoints
- Telemetry
- Emergency
- Battery Level
- Vendor Data
- Location

Step 7 Select the **Notification Triggers** check box.

Step 8 Select one or more of the following Notification trigger options:

- Chokepoints
- Telemetry
- Emergency
- Battery Level
- Vendor Data
- Location Recalculation

Step 9 Enter the IP address and port for the system that is to receive the northbound notifications.

Step 10 Choose the transport type from the drop-down list.

Step 11 Select **HTTPS** if you want to use HTTPS protocol for secure access to the destination system.

Step 12 To modify the notification parameter settings, enter the new value in the appropriate text box in the Advanced tab of the page. Table 11-9 describes each parameter.

Table 11-9 User-Configured Conditional and Northbound Notifications Parameters

Field	Configuration Options
Rate Limit	Enter the rate in milliseconds at which the mobility services engine generates notifications. A value of 0 (default) means that the mobility services engine generates notifications as fast as possible (Northbound notifications only).
Queue Limit	Enter the event queue limit for sending notifications. The mobility services engine drops any event preceding this limit. Default values: Cisco 3350 (30000), Cisco 3310 (5,000), and Cisco 2710 (10,000).
Retry Count	Enter the number of times to generate an event notification before the refresh time expires. This field can be used for asynchronous transport types which do not acknowledge the receipt of the notification and there is a possibility that the notification might be lost in transit. Default value is 1. **Note** The mobility services engine does not store events in its database.
Refresh Time	Enter the wait time in minutes that must pass before a notification is resent. For example if a device is configured for In Coverage Area notification and it is constantly being detected within the Coverage Area. The notification is sent once every refresh time.
Drop Oldest Entry on Queue Overflow	(Read-only). The number of event notifications dropped from the queue since startup.
Serialize Events per Mac address per Destination	Select this option if you want the successive events for the same MAC address to be sent to a single destination in a serial manner.

Step 13 Click **Save**.

Viewing Tag Engine Status

To access the Tag Engine Status page, choose **Services** > **Mobility Services** > *MSE Name* > **Context Aware Service** > **Tag Engine** > **Status**.

Note This option appears only if Partner Tag engine was chosen as the engine.

If tag licenses are available, then Aeroscout Tag Engine is enabled. Otherwise, Cisco Tag Engine is enabled by default.

If only the evaluation license is available, then the Cisco Tag Engine is enabled by default. The Tag Engine status page shows status based on whether it is a Aeroscout Tag Engine or Cisco Tag Engine.

Note The Aeroscout engine fails to start on MSE if NCS map names have special characters such as '&'.

Table 11-10 describes the fields in the Tag Engine Status page for the Aeroscout Tag Engine.

Table 11-10 Tag Engine Status Fields

Field	Description
Tag Location Engine Name	The Partner engine name, which is **aeroscout**.
Version	Version of the Aeroscout Tag Engine.
Description	Description for the Tag Engine.
Registered	Appears as True when the Aeroscout Tag Engine has established communication with the mobility services engine.
Active	Appears as True when the Aeroscout Tag Engine is up and running.
License Information	The maximum tags that are available with the Aeroscout Tag Engine.

If you selected Cisco Tag Engine for Context Aware Service, the Tag Engine Status page displays the following information.

Table 11-11 describes the fields in the Tag Engine Status page for the Cisco Tag Engine.

Table 11-11 Tag Engine Status Fields

Field	Description
Tag Location Engine Name	The Tag location engine name, which is **Cisco**.
Version	Version of the Cisco Tag Engine.
Description	Description for the Cisco Tag Engine.
Active	Displays as True when the Cisco Tag Engine is up and running.
License Information	The maximum tags that are available with the Cisco Tag Engine.

Viewing Notification Information for Mobility Services

The **Services > Context Aware Notifications** page provides the ability to define events. This section contains the following topics:

- Viewing the Notifications Summary for Mobility Services, page 11-69
- Viewing and Managing Notifications Settings for Mobility Services, page 11-71
- Viewing Notification Statistics, page 11-71

Viewing the Notifications Summary for Mobility Services

To view the Notification Summary, choose **Services > Context Aware Notifications > Summary**.

The mobility service sends event notifications and does not store them (fire and forget). However, if NCS is a destination of notification events, it stores the notifications it receives and groups them into the following seven categories:

- Absence (Missing)—Generated when the mobility service cannot see the asset in the WLAN for the specified time.
- Location Change Events—Generated when client stations, asset tags, rogue clients, and rogue access points move from their previous location.
- Chokepoint Notifications—Generated when a tag is seen (stimulated) by a chokepoint. This information is only reported and displayed for CCX v.1-compliant tags.
- Battery Level—Generated when a tracked asset tag hits the designated battery level.
- In/Out Area—Generated when an asset is moved inside or outside a designated area.

Note You define a containment area (campus, building, or floor) in the Maps section of NCS (Monitor > Maps). You can define a coverage area using the Map Editor.

- Movement from Marker—Generated when an asset is moved beyond a specified distance from a designated marker you define on a map.
- Emergency—Generated for a CCX v.1 compliant asset tag when the panic button of the tag is triggered or the tag becomes detached, tampered with, goes inactive or reports an unknown state. This information is only reported and displayed for CCX v.1 compliant tags.

The summary details include the following:

- All Notifications
- Client Stations
- Asset Tags
- Rogue Clients
- Rogue Access Points

Note To view details for each of the notifications, click the number under the Last Hour, Last 24 Hours, or Total Active column to open the details page for the applicable notification.

Notifications Cleared

A mobility service sends event notifications when it clears an event condition in one of the following scenarios:

- Missing (Absence)—Elements reappear.
- In/Out Area (Containment)—Elements move back in or out of the containment area.
- Distance—Elements move back within the specified distance from a marker.
- Location Changes—Clear state is not applicable to this condition.
- Battery Level—Tags are detected again operating with Normal battery level.
- Emergency
- Chokepoint

Note In NCS, the Notifications Summary page reflects whether notifications for cleared event conditions have been received.

Viewing and Managing Notifications Settings for Mobility Services

Note An Event Group must be created which contains the rules that trigger a notification.

To view the Notifications Settings, follow these steps:

Step 1 Choose **Services > Context Aware Notifications**.

Step 2 From the left sidebar menu, choose **Settings**.

Viewing Notification Statistics

You can view the notification statistics for a specific mobility services engine. To view the Notification Statistics for a specific mobility services engine, choose **Services > Mobility Services >** *MSE-name* **> Context Aware Service > Notification Statistics**.

where *MSE-name* is the name of a mobility services engine.

Table 11-12 lists and describes the fields in the Notification statistics page.

Table 11-12 Notification Statistics Fields

Field	Description
Summary	
Destinations	
Total	Total count of the destinations.
Unreachable	Count of unreachable destinations.
Notification Statistics Summary	
Track Definition Status	Status of the track definition. Track notification status can be either Enabled or Disabled.
Track Definition	Track definition can be either Northbound or CAS event notification.
Destination IP Address	The destination IP address to which the notifications are sent.
Destination Port	The destination port to which the notifications are sent.
Destination Type	The type of the destination. For example, SOAP_XML.
Destination Status	Status of the destination device. The status is either Up or Down.

Table 11-12 Notification Statistics Fields

Field	Description
Summary	
Last Sent	The date and time at which the last notification was sent to the destination device.
Last Failed	The date and time at which the notification had failed.
Total Count	The total count of notifications sent to the destination. Click the count link to view the notification statistics details of the destination device.

About Event Groups

To manage events more efficiently, you can use NCS to create event groups. Event groups help you organize your event definitions.

This section contains the following topics:

- Adding Event Groups, page 11-72
- Deleting Event Groups, page 11-72
- Working with Event Definitions, page 11-73
- Deleting an Event Definition, page 11-79

Adding Event Groups

To add an event group, follow these steps:

Step 1 Choose **Services > Context Aware Notifications**.

Step 2 Choose **Notification Definitions** from the left sidebar menu.

Step 3 From the Select a command drop-down list, choose **Add Event Group**.

Step 4 Click **Go**.

Step 5 Enter the name of the group in the Group Name text box.

Step 6 Click **Save**.

The new event group appears in the Event Settings page.

Deleting Event Groups

To delete an event group, follow these steps:

Step 1 Choose **Services > Context Aware Notifications**.

Step 2 Choose **Notification Definitions** from the left sidebar menu.

Step 3 Select the check box of the event group you want to delete.

Step 4 From the Select a command drop-down list, choose **Delete Event Group(s)**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion.

Step 7 Click **Save**.

Working with Event Definitions

An event definition contains information about the condition that caused the event, the assets to which the event applies, and the event notification destinations. This section describes how to add, delete, and test event definitions.

Note NCS enables you to add definitions on a per-group basis. Any new event definition must belong to a particular group.

To add an event definition, follow these steps:

Step 1 Choose **Services > Context Aware Notifications**.

Step 2 From the left sidebar menu, choose **Notification Definitions**.

Step 3 Click the name of the group to which you want to add the event. An event definition summary page appears for the selected event group.

Step 4 From the Select a command drop-down list, choose **Add Event Definition**.

Step 5 Click **Go**.

Step 6 Enter the name of the event definition in the Event Definition Name text box.

Note The event definition name must be unique within the event group.

Step 7 Click **Save**.

Step 8 On the General tab, manage the following parameters:

- Admin Status—Enable event generation by selecting the **Enabled** check box (disabled by default).
- Priority—Set the event priority by choosing a number from the drop-down list. Zero is highest.

  Note An event definition with higher priority is serviced before event definitions with lower priority.

- Activate—To continuously report events, choose the **All the Time** checkbox. To indicate specific days and times for activation, unselect the **All the Time** checkbox and choose the applicable days and From/Until times. Click **Save**.

Step 9 On the Conditions tab, add one or more conditions. For each condition, specify the rules for triggering event notification. To add a condition, follow these steps:

a. Click **Add** to open the Add/Edit Condition page.

b. Choose a condition type from the Condition Type drop-down list and configure its associated Trigger If parameters see (Table 11-13).

Table 11-13 Condition Type/Trigger If Parameters

Condition Type	Trigger If
Missing	Missing for Time (mins)—Enter the number of minutes after which a missing asset event is generated. For example, if you enter 10 in this text box, the mobility services engine generates a missing asset event if the mobility services engine has not located the asset for more than 10 minutes.
In/Out	Inside of or Outside of—Click **Select Area** and choose the area parameters from the Select page. Click **Select**. The area to monitor can be an entire campus, building within a campus, a floor in a building, or a coverage area (you can define a coverage area using the map editor).
Distance	In the distance of *x* (feet) from Marker text box—Enter the distance in feet that triggers an event notification if the monitored asset moves beyond the specified distance from a designated marker. Click **Select Marker** and choose the marker parameters in the Select page. Click **Select**.
Battery Level	Battery Level Is—Low, Medium, Normal. Select the appropriate battery level that triggers an event.
Location Change	An event is triggered if the location of the asset changes.
Emergency	Select **Any**, **Panic Button**, **Tampered**, or **Detached** check box.
Chokepoint	In the range of Chokepoints—Click **Select Chokepoint** check box and choose the chokepoint parameters in the Select page. Click **Select**.

c. In the Apply To drop-down list, choose the type of asset (**Any**, **Clients**, **Tags**, **Rogue APs**, **Rogue Clients** or **Interferers**) for which an event is generated if the trigger condition is met.

Note Emergency and chokepoint events are only applicable to tags (CCXv.1 compliant).

d. From the Match By drop-down list, choose the matching criteria (**MAC Address**, **Asset Name**, **Asset Group**, or **Asset Category**), the operator (**Equals** or **Like**), and enter the relevant text for the selected Match By element.

e. Click **Add**.

Step 10 On the Destination and Transport tab, follow these steps to add one or more destinations to receive event notifications and configure the transport settings:

a. Click **Add** to open the Add/Edit Destination and Transport page.

b. To add one or more new destinations, click **Add New**, enter the applicable IP address, and click **OK**.

Note The recipient system must have an event listener running to process notifications. By default, when you create an event definition, NCS adds its IP address as the destination.

c. To select a destination to receive notifications, click to highlight one or more IP addresses in the box on the right and click **Select** to add the IP address(es) to the box on the left.

d. From the Message Format field drop-down list, select **XML** or **Plain Text**.

Note If you select NCS as the destination, you must select XML format.

e. Choose one of the following transport types from the Transport Type drop-down list:

- **SOAP**—Simple Object Access Protocol. Use SOAP to send notifications over HTTP/HTTPS and to be processed by web services on the destination.

  Specify whether to send notifications over HTTPS by selecting its corresponding check box. Enter the destination port number in the Port Number text box.

- **Mail**—Use this option to send notifications through e-mail.

  Choose the protocol for sending the e-mail from the Mail Type drop-down list. Enter the following: username and password (if Authentication is enabled), name of the sender, prefix to add to the subject line, e-mail address of recipient, and a port number if necessary.

- **SNMP**—Simple Network Management Protocol. Use this option to send notifications to SNMP-capable devices.

  If you have selected SNMP version v2c then you are prompted to enter the SNMP community string in the SNMP Community text box and the applicable port number in the Port Number text box.

  If you have selected SNMP version v3 then you are prompted to enter the username, security name, choose the authentication type from the drop-down list, enter the authentication password, choose the privacy type from the drop-down list and enter the privacy password.

- **SysLog**—Specifies the system log on the destination system as the recipient of event notifications.

- Enter the notification priority in the Priority text box, the name of the facility, and the port number on the destination system.

f. Click **Add**.

Step 11 Verify that the new event definition is listed for the event group (Context Aware Service > Notifications > Event > Settings > Event Group Name).

Adding Event Definitions

An event definition contains information about the condition that caused the event, the assets to which the event applies, and the event notification destination.

The NCS enables you to add definitions for each group. An event definition must belong to a group. See the *Cisco Content-Aware Software Configuration Guide* for more information on deleting or testing event definitions.

To add an event definition, follow these steps:

Step 1 Choose **Services > Context Aware Notifications**.

Step 2 Choose **Notification Definitions** from the left sidebar menu.

Step 3 Click the name of the group to which you want to add to the event. An event definition summary page appears for the selected event group.

Step 4 From the Select a command drop-down list, choose **Add Event Definition**, and click **Go**.

Step 5 On the Conditions tab, add one or more conditions. For each condition you add, specify the rules for triggering event notifications.

Tip For example, to keep track of heart monitors in a hospital, you can add rules to generate event notifications when a heart monitor is missing for one hour, a heart monitor moves off its assigned floor, or a heart monitor enters a specific coverage area within a floor.

To add a condition, follow these steps:

a. Click **Add** to add a condition that triggers this event.

b. In the Add/Edit Condition dialog box, follow these steps:

1. Choose a condition type from the Condition Type drop-down list.

   If you chose Missing from the Condition Type drop-down list, enter the number of minutes after which a missing asset event is generated. For example, if you enter 10 in this text box, the mobility service engine generates a missing asset event if the mobility service engine has not found the asset for more than 10 minutes. Proceed to Step c.

   If you chose In/Out from the Condition Type drop-down list, choose **Inside of** or **Outside of**, then select **Select Area** to select the area to monitor for assets going into it or out of it. In the Select dialog box, choose the area to monitor, then click **Select**. The area to monitor can be an entire campus, building within a campus, a floor in a building, or a coverage area (you can define a coverage area using the map editor). For example, to monitor part of a floor in a building, choose a campus from the Campus drop-down list, choose a building from the Building drop-down list, and choose the area to monitor from the Floor Area drop-down list. Then click **Select**. Proceed to Step c.

   If you chose Distance from the Condition Type drop-down list, enter the distance in feet that triggers an event notification if the monitored asset moves beyond the specified distance from a designated marker, then click **Select Marker**. In the Select dialog box, choose the campus, building, floor, and marker from the corresponding drop-down list, and click **Select**. For example, if you add a marker to a floor plan and set the distance in the Trigger. If the text box is set to 60 feet, an event notification is generated if the monitored asset moves more than 60 feet away from the marker. Proceed to Step c.

   Note You can create markers and coverage areas using the Map Editor. When you create marker names, make sure they are unique across the entire system.

   If you chose Battery Level from the Condition Type drop-down list, select the check box next to the battery level (low, medium, normal) that triggers an event. Proceed to Step c.

If you chose Location Change from the Condition Type drop-down list, proceed to Step c.

If you chose Emergency from the Condition Type drop-down list, click the button next to the emergency (any, panic button, tampered, detached) that triggers an event. Proceed to Step c.

If you chose Chokepoint from the Condition Type drop-down list, proceed to Step c. There is only one trigger condition, and it is displayed by default. No configuration is required.

c. From the Apply To drop-down list, choose the type of asset (Any, Clients, Tags, Rogue APs, Rogue Clients, or Interferers) for which an event is generated if the trigger condition is met.

Note If you choose the any option from the Apply to drop-down list, the battery condition is applied to all tags, clients, and rogue access points and rogue clients.

Note Emergency and chokepoint events apply only to Cisco-compatible extension tags Version 1 (or later).

d. From the Match By drop-down list, choose the matching criteria (**MAC Address**, **Asset Name**, **Asset Group**, or **Asset Category**), the operator (**Equals** or **Like**) from the drop-down list, and enter the relevant text for the selected Match By element.

Some examples of asset matching criteria that you can specify:

- If you choose **MAC Address** from the Match By drop-down list, choose **Equals** from the Operator drop-down list, and enter a MAC address (for example, 12:12:12:12:12:12), the event condition applies to the element whose MAC address is 12:12:12:12:12:12 (exact match).
- If you choose **MAC Address** from the Match By drop-down, choose **Like** from the Operator drop-down list, and enter **12:12**, the event condition applies to elements whose MAC address starts with 12:12.

e. Click **Add** to add the condition you have just defined.

Note If you are defining a chokepoint, you must select the chokepoint after you add the condition.

To select a chokepoint, do the following:

1. Click **Select Chokepoint**. An entry page appears.
2. Choose **Campus**, **Building**, and **Floor** from the appropriate drop-down lists.
3. Choose a Chokepoint from the menu that appears.

You are returned to the Add/Edit Condition page, and the location path (Campus > Building > Floor) for the chokepoint auto-populates the text area next to the Select Checkpoint button.

Step 6 On the Destination and Transport tab, follow these steps to add one or more destinations to receive event notifications and to configure the transport settings:

a. To add a new destination, click **Add**. The Add/Edit Destination configuration page appears.

b. Click **Add New**.

c. Enter the IP address of the system that receives event notifications, and click **OK**.

The recipient system must have an event listener running to process notifications. By default, when you create an event definition, NCS adds its IP address as the destination.

d. To select a destination to send event notifications to, highlight one or more IP addresses in the box on the right, and click **Select** to add the IP addresses to the box on the left.

e. Choose **XML** or **Plain Text** to specify the message format.

f. Choose one of the following transport types from the Transport Type drop-down list:

- **SOAP**—Specifies Simple Object Access Protocol, a simple XML protocol, as the transport type for sending event notifications. Use SOAP to send notifications over HTTP/HTTPS that are processed by web services on the destination.

  If you choose SOAP, specify whether to send notifications over HTTPS by selecting its corresponding check box. If you do not, HTTP is used. Also, enter the destination port number in the Port Number text box.

- **Mail**—Use this option to send notifications through e-mail.

  If you choose Mail, you need to choose the protocol for sending the e-mail from the Mail Type drop-down list. You also need to enter the following information: username and password (if Authentication is enabled), name of the sender, prefix to add to the subject line, e-mail address of recipient, and a port number if necessary.

- **SNMP**—Use Simple Network Management Protocol, a very common technology for network monitoring used to send notifications to SNMP-capable devices.

  If you choose SNMP, enter the SNMP community string in the SNMP Community text box and the port number to send notifications to in the Port Number text box.

- SysLog—Specifies the system log on the destination system as the recipient of event notifications.

  If you choose SysLog, enter the notification priority in the Priority text box, the name of the facility in the Facility text box, and the port number of the destination system in the Port Number text box.

g. To enable HTTPS, select the **Enable** check box next to it.

Port Number auto-populates.

h. Click **Save**.

Step 7 On the General tab, follow these steps:

a. Select the **Enabled** check box for Admin Status to enable event generation (disabled by default).

b. Set the event priority by choosing a number from the Priority drop-down list. Zero is the highest priority.

Note An event notification with high priority is serviced before event definitions with lower priority.

c. To select how often the event notifications are sent:

1. Select the **All the Time** check box to continuously report events. Proceed to Step g.
2. Unselect the **All the Time** check box to select the day and time of the week that you want event notifications sent. Days of the week and time fields appear for the selection. Proceed to Step d.

d. Select the check box next to each day you want the event notifications sent.

e. Select the time for starting the event notification by selecting the appropriate hour, minute, and AM/PM options from the Apply From heading.

f. Select the time for ending the event notification by selecting the appropriate hour, minute, and AM/PM options from the Apply Until heading.

g. Click **Save**.

Step 8 Verify that the new event notification is listed for the event group (Mobility > Notifications > Settings > Event Group Name).

Deleting an Event Definition

To delete one or more event definitions from NCS, follow these steps:

Step 1 Choose **Services > Context Aware Notifications**.

Step 2 From the left sidebar menu, choose **Settings**.

Step 3 Click the name of the group from which you want to delete the event definitions.

Step 4 Select the event definition that you want to delete by selecting its corresponding check box.

Step 5 From the Select a command drop-down list, choose **Delete Event Definition(s)**.

Step 6 Click **Go**.

Step 7 Click **OK** to confirm that you want to delete the selected event definitions.

Client Support on MSE

You can use the NCS advanced search feature to narrow the client list based on specific categories and filters. See the "Using the Search Feature" section on page 2-33 section or the "Advanced Search" section on page 2-34 for more information.You can also filter the current list using the Show drop-down list. See the " Filtering Clients and Users" section on page 9-11 for more information.

This section contains the following topics:

Searching a Wireless Client from NCS on MSE by IPv6 Address

Note Only wireless clients have IPv6 addresses in this release.

To search for a MSE located clients using the NCS Advanced search feature, follow these steps:

Step 1 Click **Advanced Search** located in the top right corner of the NCS UI

Step 2 In the New Search dialog, choose **Clients** as the search category from the Search Category drop-down list.

Step 3 From the Media Type drop-down list, choose **Wireless Clients**.

Note The Wireless Type drop-down list appears only when you choose Wireless Clients as the media type.

Step 4 From the Wireless Type drop-down list, choose any of the following types: **All**, **Lightweight or Autonomous Clients**.

Step 5 From the Search By drop-down list, choose **IP Address**.

Note Searching a client by IP address can contain either full or partial IP address. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

Step 6 From the Clients Detected By drop-down list, choose clients detected by as MSE.

This displays clients located by Context-Aware Service in the MSE by directly communicating with the controllers.

Step 7 From the Last detected within drop-down list, choose the time within which the client was detected.

Step 8 Enter the client IP address in the Client IP Address text box. You can enter wither a partial or full IPv6 address.

Note If you are searching for the client from NCS on the MSE by IPv4 address, enter the IPv4 address in the Client IP address text box.

Step 9 From the Client States drop-down list, choose the client states. The possible values for wireless clients are **All States**, **Idle**, **Authenticated**, **Associated**, **Probing**, or **Excused**. The possible values for wired clients are **All States**, **Authenticated**, and **Associated**.

Step 10 From the Posture Status drop-down list, choose the posture status to know if the devices are clean or not. The possible values are **All**, **unknown**, **Passed**, **and Failed**.

Step 11 Select the **CCX Compatible** check box to search for clients that are compatible with Cisco Client Extensions. The possible values are **All Versions**, **V1**, **V2**, **V3**, **V4**, **V5**, and **V6**.

Step 12 Select the **E2E Compatible** check box to search for clients that are end to end compatible. The possible values are **All Versions**, **V1**, and **V2**.

Step 13 Select the **NAC State** check box to search for clients identified by a certain Network Admission Control (NAC) state. The possible values are **Quarantine**, **Access**, **Invalid**, and **Not Applicable**.

Step 14 Select the **Include Disassociated** check box to include clients that are no longer on the network but for which NCS has historical records.

Step 15 From the **Items per page** drop-down list, choose the number of records to be displayed in the search results page.

Step 16 Select the **Save Search** check box to save the selected search option.

Step 17 Click Go.

The Clients and Users page appears with all the clients detected by the MSE.

Viewing the Clients Detected by MSE

To view all the clients detected by MSE, follow these steps:

Step 1 Choose **Monitor > Clients and Users** to view both wired and wireless clients information.

The Client and Users page appears.

The Clients and Users table displays a few column by default. If you want to display the additional columns that are available, click , and then click **Columns**. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.

Step 2 Filter the current list to choose all the clients that are detected by MSE by choosing **Clients detected by MSE** from the Show drop-down list.

All the clients detected by MSE including wired and wireless appear.

The following different parameters are available in the Clients Detected by MSE table:

- MAC Address—Client MAC address.
- IP Address—Client IP address.

  The IP Address that appears in the IP Address column is determined by a predefined priority order. The first IP address available in the following order appears in the IP address text box:

  – IPv4 address

  Note Only wireless clients have IPv6 addresses in this release. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

  – IPv6 global unique address. If there are multiple addresses of this type, most recent IPv6 address that the client received is shown, because a user could have two Global IPv6 addresses but one might have been from an older Router Advertisement that is being aged out.

  – IPv6 local unique address. If there are multiple IPv6 local unique addresses, then the most recent address appears.

  – IPv6 link local address. For an IPv6 client it always have at least a link local address.

  The following are the different IPv6 address types:

  – Link-local Unicast—The link-local addresses are designed to be used for addressing on a single link for purposes such as auto-address configuration, neighbor discovery, or when no routers are present.

  – Site-local Unicast—The site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix.

  – Aggregatable Global Unicast—The aggregatable global unicast address uniquely identifies the client in global network and equivalent to public IPv4 address. A client can have multiple aggregatable global unicast addresses.

- IP Type—The IP address type can be IPv4 and IPv6.

  – Global Unique

  – Unique Local

  – Link Local

- User Name—Username based on 802.1x authentication. Unknown is displayed for client connected without a username.
- Type—Indicates the client type.

  – indicates a lightweight client

  -  indicates a wired client
  -  indicates an autonomous client
- Vendor—Device vendor derived from OUI.
- Device Name—Network authentication device name. For example, WLC and switch.
- Location—Map location of the connected device.
- VLAN—Indicates the access VLAN ID for this client.
- Status—Current client status.
  - Idle—Normal operation; no rejection of client association requests.
  - Auth Pending—Completing a AAA transaction.
  - Authenticated—802.11 authenticated complete.
  - Associated—802.11 association complete. This is also used by wired clients to represent that a client is currently connected to the network.
  - Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.
  - To Be Deleted—The client is deleted after disassociation.
  - Excluded—Automatically disabled by the system due to perceived security threat.
- Interface—Controller interface (wireless) or switch interface (wired) that the client is connected to.
- Protocol
  - 802.11—wireless
  - 802.3—wired
- Association Time—Last association start time (for wireless client). For a wired client, this is the time when a client is connected to a switch port. This is blank for a client which is associated but has problems being on the network.
- CCX—Lightweight wireless only.

Step 3 Select the radio button next to MAC Address in the Client and User page to view the associated client information. The following are the different client parameters that appear.

- Client Attributes
- Client IPv6 Addresses
- Client Statistics

Note Client Statistics shows the statistics information after the client details are shown.

- Client Association History
- Client Event Information
- Client Location Information
- Wired Location History
- Client CCX Information

Client Attributes

When you select a client from the Clients and Users list, the following client details are displayed. Clients are identified using the MAC address.

These following details are displayed:

- General—Lists the following information:
  - User Name
  - IP Address
  - MAC address
  - Vendor
  - Endpoint Type
  - Client Type
  - Media Type
  - Mobility Role
  - Hostname
  - E2E
  - Power Save
  - CCX
  - Foundation Service
  - Management Service
  - Voice Service
  - Location Service

Note Click the icon next to the username to access the correlated users of a user.

- Session—Lists the following client session information:
  - Controller Name
  - AP Name
  - AP IP Address
  - AP Type
  - AP Base Radio MAC
  - Anchor Address
  - 802.11 State
  - Association ID
  - Port
  - Interface
  - SSID
  - Profile Name
  - Protocol

  - VLAN ID
  - AP Mode
- Security (wireless and Identity wired clients only)—Lists the following security information:
  - Security Policy Type
  - EAP Type
  - On Network
  - 802.11 Authentication
  - Encryption Cipher
  - SNMP NAC State
  - RADIUS NAC State
  - AAA Override ACL Name
  - AAA Override ACL Applied Status
  - Redirect URL
  - ACL Name
  - ACL Applied Status
  - FlexConnect Local Authentication
  - Policy Manager State
  - Authentication ISE
  - Authorization Profile Name
  - Posture Status
  - TrustSec Security Group
  - Windows AD Domain

Note The identity clients are the clients whose authentication type is 802.1x, MAC Auth Bypass or Web Auth. For non-identity clients, the authentication type is N/A.

Note The data that appears under the client attributes differs based on identity and non-identity clients. For identity clients, you can see the security information such as Authentication status, Audit Session ID, and so on.

- Statistics (wireless only)
- Traffic—Shows the client traffic information.
- For wireless clients, client traffic information comes from controller. For wired clients, the client traffic information comes from ISE, and you must enable accounting information and other necessary functions on switches.

Statistics

The Statistics group box contains the following information for the selected client:

- Client AP Association History

- Client RSSI History (dBm)—History of RSSI (Received Signal Strength Indicator) as detected by the access point with which the client is associated.
- Client SNR History—History of SNR (signal-to-noise Ratio of the client RF session) as detected by the access point with which the client is associated.
- Bytes Sent and Received (Kbps)—Bytes sent and received with the associated access point.
- Packets Sent and Received (per sec)—Packets sent and received with the associated access point.
- Client Data rate

Note Hover your mouse cursor over points on the graph for additional statistical information.

This information is presented in interactive graphs. See the "Interactive Graphs" section on page 8-248 for more information.

Client IPv6 Addresses

The IPv6 address group box contains the following information for the selected client:

- IP Address—Shows the clients IPv6 address.
- Scope—Contains 3 types scope. They are Global Unique, Local Unique, and Link Local.
- Address Type—Shows the address type.
- Discovery Time—Time when the IP was discovered.

Association History

The association history dashlet shows information regarding the last ten association times for the selected client. This information helps in troubleshooting the client.

The Association History dashlet contains the following information:

- Association Time
- Duration
- User Name
- IP Address
- IP Address Type
- AP Name
- Controller Name
- SSID

Events

The Event group box of the Client Details page display all events for this client including the event type as well as the date and time of the event.

- Event Type
- Event Time
- Description

Map

Click **View Location History** to view location history details of wired and wireless clients.

You can view the location details for wired and wireless clients.

The following location history information is displayed for a wired or wireless client:

- Timestamp
- State
- Port Type
- Slot
- Module
- Port
- User Name
- IP Address
- Switch IP
- Server Name
- Map Location Civic Location

Upgrading from 5.0 to 6.0 or 7.0

Caution The number of supported clients, tags, and access points (wIPS) is reset to 100 clients, 100 tags, and 20 access points when you upgrade to Release 6.0 or later. All tracking beyond these limits is lost. These limits correspond to the 60-day evaluation licenses that are standard.

Caution When upgrading the mobility services engine from 6.0 to 7.0, if any limits have been set on wireless clients or rogues, they are reset because of the wired client limit change in 7.0.

Caution You must back up the mobility services engine database before upgrading from release 5.1 or 6.0 to 7.0 to preserve client, tag, and access point configurations. You can restore the database after the software upgrade.

Note Release 5.1 did not support licenses. You must order, register, and install licenses to track client and tag locations (CA) or access points (wIPS) beyond the limits of the 60-day evaluation licenses.

To upgrade to release 7.0, follow these steps:

Step 1 Register the Product Authorization Key (PAK).

Note You receive a PAK when you order a license. If you have lost your PAK, you can use your sales order or the UDI number of the mobility services engine to register.

- Client and wIPS licenses are registered at: www.cisco.com/go/license
- Tag licenses are registered at: http://www.aeroscout.com/content/support

Step 2 Back up the mobility services engine database:

a. Choose **Services > Mobility Services**.

b. Click the name of the mobility services engine on which you want to back up.

c. Choose **System > Maintenance.**

d. Click **Backup**.

e. Enter the name of the backup file.

f. Click **Submit** to backup the historical data to the hard drive of the server running the NCS.

Step 3 Download release 7.0:

a. Choose **Services > Mobility Services**.

b. Click the name of the mobility services engine to which you want to download the software.

c. Choose **System > Maintenance > Download Software** from the left sidebar menu.

d. To download software, do one of the following:

– To download software listed in the NCS directory, select the **Select from uploaded images to transfer** into the Server radio button. Choose a binary image from the drop-down list.

NCS downloads the binary image to the FTP server directory you specified during the NCS installation.

– To use downloaded software available locally or over the network, select the **Browse a new software image to transfer into the Server** radio button and click **Choose File**. Locate the file and click **Open**.

e. Click **Download** to send the software to the /opt/installers directory on the mobility services engine.

Step 4 Install release 7.0 using the MSE CLI:

a. To overwrite existing software, enter:

```
/etc/init.d/msed stop
cd opt/installers
./<mse software file name>
```

b. To perform a fresh install, enter:

```
/etc/init.d/msed stop
cd /opt/mes/uninstall
```

./uninstall *(*enter this once in directory)

(Enter no when prompted to keep old database)

```
cd /opt/installers
./<mse software file name>
```

Step 5 Restore the mobility services engine database (For Step 4 b.):

a. Choose **Services > Mobility Services**.

b. Click the name of the mobility services engine on which you upgraded the software.

c. Choose **Maintenance > Restore** from left sidebar menu.

d. Choose the filename to restore from the drop-down list. Click **Submit**.

Step 6 Install the licenses.

See the Chapter 2 of the *ContextAware Services Configuration Guide Release 7.0* at

http://www.cisco.com/en/US/products/ps9806/products_installation_and_configuration_guides_list.html for more information.

Viewing the MSE Alarm Details

In the Monitor > Alarms page, click an MSE item under Failure Source column to access the alarms details for a particular MSE.

Alternatively, you can choose **Services** > **Mobility Services** > *MSE Name* > **System** > **Status** > **NCS Alarms** page and click a particular MSE item under Failure Source column to access the alarms details for a particular MSE.

Figure 11-2 shows a NCS alarm for MSE.

Figure 11-2 MSE Alarm

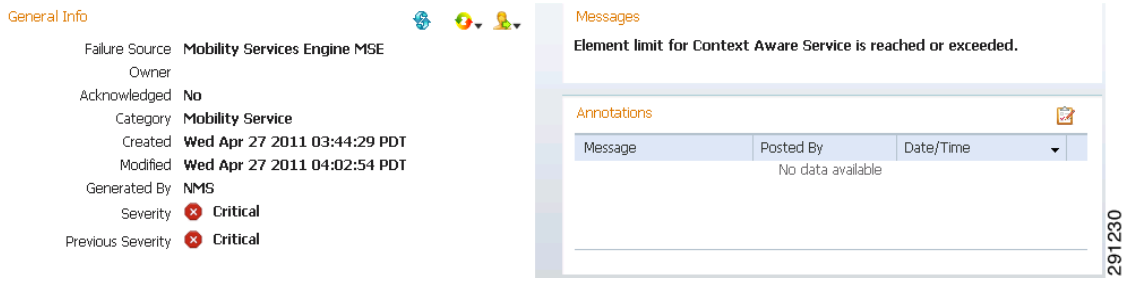


Table 11-14 describes the various fields in the Alarm Detail page for an MSE.

Table 11-14 General Parameters

Field	Description
Failure Source	The MSE that generated the alarm.
Owner	Name of person to which this alarm is assigned, or blank.
Acknowledged	Displays whether or not the alarm is acknowledged by the user.
Category	The category of the alarm.The Alarm category is Mobility Services for MSEs.
Created	Month, day, year, hour, minute, second, AM or PM alarm created.
Modified	Month, day, year, hour, minute, second, AM or PM alarm last modified.
Generated By	This field displays MSE.

Table 11-14 General Parameters (continued)

Field	Description
Severity	Level of security: Critical, Major, Minor, Warning, Clear, Info, Color coded.
Previous Severity	Critical, Major, Minor, Warning, Clear, Info. Color coded.

Note The General information might vary depending on the type of alarm. For example, some alarm details might include location and switch port tracing information.

- Annotations—Enter any new notes in this text box and click **Add** to update the alarm. Notes appear in the "Annotations" display page.
- Messages—Displays information about the alarm.
- Audit Report—Click to view config audit alarm details. This report is only available for Config Audit alarms.

  Configuration audit alarms are generated when audit discrepancies are enforced on config groups.

  Note If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group.

  The alarms have links to the audit report where you can view a list of discrepancies for each controller.

- Event History—Opens the MSE Alarm Events page to view events for this alarm. When there are multiple alarm pages, the page numbers appear at the top of the page with a scroll arrow on each side. Use these scroll arrows to view additional alarms.

Select a command

The Select a command drop-down list provides access to the following functions:

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Delete—Delete the selected alarm(s).
- Clear—Clear the selected alarm(s). Indicates that the alarm is no longer detected by any access point.

  Note Once the severity is Clear, the alarm is deleted from NCS after 30 days.

- Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in NCS and you can search for all Acknowledged alarms using the alarm search functionality. See the "Acknowledging Alarms" section on page 5-141 for more information.
- Unacknowledge—You can choose to unacknowledge an already acknowledged alarm.

- Email Notification—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications. See the "Monitoring RFID Tags" section on page 5-118 for more information.
- Event History—Takes you to the Monitor > Events page to view events for this alarm. See the "Monitoring Events" section on page 5-149 for more information.

See the "Monitoring Alarms" section on page 5-131 for more information on Alarms.

MSE License Overview

The MSE packages together multiple product features related to network topology, design such as NMSP, Network Repository along with related Service Engines, and application processes, such as the following:

- Context-Aware Service
- Wireless Intrusion Prevention System (WIPS)

To enable smooth management of MSE and its services, various licenses are offered.

Note You must have a Cisco NCS license to use MSE and its associated services.

This section contains the following topics:

MSE License Structure Matrix

Table 11-15 lists the breakdown of the licenses between the High end, Low end and Evaluation licenses for MSE, Location services, SCM, wIPS and MIR.

Table 11-15 MSE License Structure Matrix

	High End	Low End	Evaluation
MSE Platform	High-end appliance and infrastructure platform such as the Cisco 3350 and 3355 mobility services engines.	Low-end appliance and Infra-structure platform such as Cisco 3310 mobility services engine.	—
Context Aware Service	18,000 Tags	2000 Tags	Validity 60 days, 100 Tags and 100 Elements.
	18,000 Elements	2000 Elements	
wIPS	3000 access points	2000 access points	Validity 60 days, 20 access points.

Sample MSE License File

The following is a sample MSE license file:

```
FEATURE MSE cisco 1.0 permanent uncounted \
```

```
VENDOR_STRING=UDI=udi,COUNT=1 \
HOST ID=ANY \
NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</LicLineID> \
<PAK>dummyPak</PAK>" \
SIGN="0C04 1EBA BE34 F208 404F 98ED 43EC \
45D7 F881 08F6 7FA5 4DED 43BC AF5C C359 0444 36B2 45CF 6EA6 \
1DB1 899F 413F F543 F426 B055 4C7A D95D 2139 191F 04DE"
```

This sample file has 5 license entries. The first word of the first line of any license entry tells you what type of license it is. It can either be a Feature or Increment license. A feature license is a static lone item to license. There can be multiple services engines running in MSE. An Increment license is an additive license. In MSE, the individual service engines are treated as increment licenses.

The second word of the first line defines the specific component to be licensed. For example, MSE, LOCATION_TAG. The third word depicts the vendor of the license, for example Cisco. The fourth word denotes the version of the license, example 1.0. The fifth word denotes the expiration date, this can be permanent for licenses that never expire or a date in the format dd-mm-yyyy. The last word defines whether this license is counted.

See the "Mobility Services Engine (MSE) License Information" section on page 15-136 for more information on the license types.

Revoking and Reusing an MSE License

You can revoke an MSE appliance license from one system and reuse it on another system. When you revoke a license, the license file is deleted from the system. If you want to reuse the license on another system, then the license needs to be rehosted.

If you want to reuse a license with an upgrade SKU on another system, then you must have the corresponding base license SKU installed in the system to which you want to reuse the upgrade SKU. You cannot reuse the upgrade license SKU in a system if the corresponding base license SKU is deleted from it.

When you revoke a license, MSE restarts the individual service engines to reflect the changes to the licenses. Then the service engines receives the updated capacity from MSE during startup.

See the following sections for more information on Licensing:

- NCS License Information, page 15-132
- Mobility Services Engine (MSE) License Information, page 15-136
- Mobility Services Engine (MSE) License Summary, page 15-137

Deploying the MSE Virtual Appliance

MSE is also offered as a virtual appliance. The MSE virtual appliance software is distributed as an Open Virtualization Archive (OVA) file.

Note See the VMware cSphere 4.0 documentation for more information about setting up your VMware environment.

Note See the *Cisco Prime Network Control System. Getting Started Guide, Release 1.0* for more information on the physical appliance.

When the MSE is located on the physical appliance, the license installation process is based on Cisco UDI (Unique Device Identifier). Choose **Administration > License Center** on the NCS UI to add the license. When the MSE is located on the virtual appliance, the license installation is done using a VUDI (Virtual Unique Device Identifier) instead of UDI.

Note MSE is available as a virtual appliance for this release and later. Virtual appliance must be activated first before installing any other service licenses.

For a virtual appliance, you must have an activation license. Without an activation license, if MSE starts in evaluation mode even if the licenses are present on the host, it rejects the permanent license if the activation license is not installed. If the virtual appliance is added to NCS, NCS does not allow MSE to be synchronized unless the activation license is added to the MSE.

Note Virtual licenses are not allowed on physical appliances.

You can add and delete a virtual appliance license either using the **Services > Mobility Services Engine > Add Mobility Services Engine** page when you are installing MSE for the first time or you can use **Administration > License Center** page to add or delete a license.

See the "Adding a License File to MSE Using the License Center" section on page 11-92 and the "Deleting an MSE License File" section on page 11-8 for more information on adding a license and deleting a license using the Mobility Services Engine wizard.

This section contains the following topics:

Adding a License File to MSE Using the License Center

To add a license, follow these steps:

Step 1 Install the MSE virtual appliance.

Step 2 Add MSE to NCS using the "Adding a Mobility Services Engine" section on page 11-6.

Step 3 Choose **Administration > License Center** on the NCS UI to access the License Center page.

Step 4 Choose **Files > MSE Files** from the left sidebar menu.

Step 5 Click **Add** to add a license.

The Add A License File menu appears.

Step 6 Select the MSE and browse to the activation license file.

Step 7 Click Submit.

Once you submit, the license is activated and license information appears in the License Center page.

Viewing the MSE License Information using License Center

The license center allows you to manage NCS, Wireless LAN Controllers, and MSE licenses. To view the license information, follow these steps

Step 1 Choose **Administration > License Center** to access the License Center page.

Step 2 Choose **Summary > MSE** from the left sidebar menu, to view the summary page.

The MSE Summary page displays the following information. See Table 11-16.

Table 11-16 General Parameters

Field	Description
MSE Name	Provides a link to the MSE license file list page.
Service	Type of service using: CAS or wIPS.
Platform Limit	Platform limit.
Type	Specifies the type of MSE.
Installed Limit	Displays the total number of client elements licensed across MSEs.
License Type	The three different types of licenses. They are permanent, evaluation, and extension.
Count	The number of CAS or wIPS elements currently licensed across MSEs.
Unlicensed Count	Displays the number of client elements that are not licensed.
%Used	The percentage of CAS or wIPS elements licensed across MSEs.

Removing a License File Using the License Center

To remove a license, follow these steps:

Step 1 Install the MSE virtual appliance.

Step 2 Add MSE to NCS using the wizard.

Step 3 Choose **Administration > License Center** on NCS UI to access the License Center page.

Step 4 Choose **Files > MSE Files** from the left sidebar menu.

Step 5 Choose an MSE license file that you want to remove by selecting the radio button, and click **Remove**.

Step 6 Click **OK** to confirm the deletion.

Location Assisted Client Troubleshooting from the Context Aware Dashboard

You can use the Context Aware dashboard on the NCS home page to troubleshoot a client.

You can specify a MAC address or Username or IP address as the search criteria, and click **Troubleshoot**.

Note Username, IP address, and partial MAC address-based troubleshooting is supported only on MSEs Version 7.0.200.0 and later.

The Troubleshoot Client page appears.

You can view the Context Aware History report on the Context Aware History tab.

You can filter this report based on MSE Name. You can further filter the report based on Timezone, State or All. The states can be either associated or dissociated.

If you select timezone then you can select any of the following:

- Date and Time

Or

- Any one of these values from the drop-down list:
  - Last 1 Hour
  - Last 6 Hours
  - Last 1 Day
  - Last 2 Days
  - Last 3 Days
  - Last 4 Days
  - Last 5 Days
  - Last 6 Days
  - Last 7 Days
  - Last 2 Weeks
  - Last 4 Weeks

Alternately, you can use the Generate Report link to generate a Client Location History report. You can also opt to export to CSV or PDF format or e-mail the report using the icons available in the report page.

See the "Context Aware Dashboard" section on page 2-21 for more information on the Context Aware dashboard of the NCS home page.

MSE

You can generate many Context Aware reports using the Report Launch Pad. See the "ContextAware Reports" section on page 14-78 for more information on Context Aware reports.

Monitoring Maps

Maps provide a summary view of all your managed system on campuses, buildings, outdoor areas, and floors. See the "Monitoring Maps" section on page 4-8 for more information on maps.

Planning for and Configuring Context-Aware Software

Context-Aware Software (CAS) resides on the mobility services engine. For more information on the CAS service, see the *Cisco Context-Aware Software Configuration Guide.*

Note If you have a location server, you can track or map non-Cisco CCX tags.

Note Context-Aware Software was previously referred to as *Cisco location-based services*.

Chapter 4 of the *Cisco Context-Aware Software Configuration Guide* contains the following information on configuring and viewing system properties on the mobility services engine:

- Configuring general properties
- Modifying NMSP parameters
- Viewing active sessions on a system
- Adding and deleting trap destinations
- Viewing and configuring advanced parameters

Chapter 5 of the *Cisco Context-Aware Software Configuration Guide* contains information on configuring and managing users and groups on the mobility services engine.

Chapter 6 of the *Cisco Context-Aware Software Configuration Guide* contains the following information on event notifications:

- Adding and deleting event groups
- Adding, deleting, and testing event definitions
- Viewing event notification summary
- Notifications cleared
- Notification message formats

Chapter 7 of the *Cisco Context-Aware Software Configuration Guide* contains the following information on the tools and configurations that can be used to enhance the location accuracy of elements (clients, tags, rogue clients, interferers and rogue access points):

- Planning for data, voice, and location deployment
- Creating and applying calibration models
- Inspecting location readiness and quality
- Inspecting location quality using calibration data
- Verifying location accuracy
- Using chokepoints to enhance tag location reporting
- Using Wi-Fi TDOA receiver to enhance tag location reporting
- Using tracking optimized monitor mode to enhance tag location reporting
- Defining inclusion and exclusion regions on a floor
- Defining a rail line on a floor
- Modifying context aware software parameters
- Enabling Location Services on Wired Switches and Wired Clients.
- Assigning a Catalyst Switch to Mobility Services Engine and Synchronizing

Chapter 8 of the *Cisco Context-Aware Software Configuration Guide* contains the following information on how to monitor the mobility services engine by configuring and viewing alarms, events, and logs and how to generate reports on system utilization and element counts:

- Working with alarms
- Working with events
- Working with logs
- Generating reports
- Monitoring wireless clients
- Monitoring tagged assets
- Monitoring chokepoints
- Monitoring Wi-Fi TDOA receivers
- Monitoring Wired Switches
- Monitoring Wired Clients
- Monitoring Interferers

Chapter 9 of the *Cisco Context-Aware Software Configuration Guide* contains the following information on backing up and restoring mobility services engine data and updating the mobility services engine software:

- Recovering a lost password
- Recovering a lost root password
- Backing up and restoring mobility services engine data
- Downloading software to mobility services engines
- Configuring the NTP server
- Defragmenting the mobility services engine database

- Rebooting the mobility services engine hardware
- Shutting down the mobility services engine hardware
- Clearing mobility services engine configurations

wIPS Planning and Configuring

With a fully integrated solution, Cisco can continually monitor wireless traffic on both the wired and wireless networks and can use that network intelligence to analyze attacks from many different sources of information to more accurately pinpoint and proactively prevent attacks versus waiting until damage or exposure has occurred. See the *Cisco Adaptive Wireless IPS* documentation for the following information:

- NCS and wIPS integration overview
- Mobility services engines
- wIPS profiles
- Configuring SSID group list
- Viewing wIPS alarms
- Viewing wIPS events
- Configuring access points and access point templates
- policy alarm encyclopedia
- NCS security vulnerability assessment
- Rogue management
- Radio resource management

MSAP

Cisco Mobility Services Advertisement Protocol (MSAP) provides requirements for MSAP client and server and describes the message exchanges between them. Mobile devices can retrieve service advertisements from MSAP server over Wi-Fi infrastructure using MSAP. MSAP is introduced in this release of the Mobility Services Engine (MSE) and provides server functionality.

MSAP is used by the mobile devices that have been configured with a set of policies for establishing network connectivity. MSAP facilitates mobile devices to discover network based services available in a local network or services that are enabled through service providers. MSAP provides service advertisements, that describe available services to the mobile devices. Once the mobile device receives the service advertisements, it displays their icon and data on its user interface. You can launch the advertised service by clicking the displayed icon.

This section contains the following information:

- Licensing for MSAP, page 11-98
- Provisioning MSAP Service Advertisements, page 11-98
- Deleting Service Advertisements, page 11-99
- Applying Service Advertisements to a Venue, page 11-100
- Viewing the Configured Service Advertisements, page 11-100

Licensing for MSAP

The MSAP license is based on the number of service advertisements supported by the MSE. There are two types of MSAP license: the evaluation license and permanent license. The evaluation license is valid for 60 days and the permanent license is based on the MSE platform and the number of service advertisements supported.

Provisioning MSAP Service Advertisements

To add new MSAP advertisements, follow these steps:

Step 1 Choose **Services > MSAP**.

Step 2 From the Select a command drop-down list, choose **Add Service Advertisements**, and click **Go**.

The Service Advertisement Details page appears.

Step 3 Enter the service provider name in the Provider Name text box. It is the name of the provider who wants to provide advertisements to the client.

Step 4 Select an icon that is associated with the service provider by clicking the **Choose File**. This is the icon that is displayed on the client handset.

Adding Venue Policy to Service Advertisements

Note You can also apply service advertisements to a venue by choosing Services > MASP on the NCS UI. See the "Applying Service Advertisements to a Venue" section on page 11-100 for more information on how to apply service advertisements.

Step 5 Click **Add Venue** to specify at which venues you want the advertisements to be broadcasted on.

The Add/Edit Venue page appears.

Step 6 Enter the venue name in the Venue Name text box.

Step 7 From the Area Type drop-down list, choose the area type where you want to display the service advertisements. The possible values are **Floor Area** and **Outdoor area**.

Step 8 From the Campus drop-down list, choose the campus type where you want to display the service advertisements. The possible values are **System Campus** and **Site 5**.

Step 9 From the Building drop-down list, choose the building name where you want the advertisements to appear.

Step 10 From the Floor drop-down list, choose the floor type.

Note Depending on what floor you choose, the information in the Display near selected APs information changes.

Step 11 From the SSID drop-down list, choose SSIDs on which you want to broadcast the service advertisements. You can choose multiple SSIDs.

Step 12 Select the Display Rule radio button. You can select either the **Display everywhere** or **Display near selected APs** radio button. By default, Display everywhere radio button is selected.

If you select the Display everywhere radio button, then it searches for all the MSAP supported controllers that provide these SSID and assign these controllers to the MSE.

- If you select the Display everywhere radio button, then it searches for all the MSAP supported controllers that provide SSIDs and assigns these controllers to the MSE.

If you select the Display near selected APs radio button, then you can configure the following parameters:

- AP—Select those APs on which you want the advertisements to broadcast.
- Radio—Select the radio frequency on which you want the advertisements to be broadcasted on. The service advertisement is displayed when the mobile device is near the radio band that you have selected. The possible values are 2.4 GHz or 5 GHz.
- min RSSI—Enter a value for RSSI at which you want the service advertisements to display on the user interface.

Step 13 Click **Save** to add the venue. The venue is added to the list of venues on the Service Advertisement Details page.

Adding Service Brief Information to the Service Advertisement

Step 14 Click **Add Advertisement**.

The Add/Edit Advertisement page appears.

Step 15 From the Advertisement Type drop-down list, choose the type of advertisement you want to display.

Step 16 Enter the name that you want to display on the handset in the Friendly Name text box.

Step 17 Enter the service description in the Friendly Description text box.

Step 18 Enter the URL for each type of handset. The URL identifies the location at which the service can be retrieved. You can add multiple URLs by clicking **Add More URL**.

Step 19 Click **Save**. This information is applied to the MSE and the synchronization happens automatically.

Deleting Service Advertisements

To delete a service advertisement, follow these steps:

Step 1 Choose **Services > MSAP**.

The MSAP page appears.

Step 2 Select the check box of the service advertisement that you want to delete.

Step 3 From the Select a command drop-down list, choose **Delete Service Advertisement**, and click **Go**, or Click **Delete** in the MSAP page.

Step 4 Click **OK** to confirm the deletion.

Applying Service Advertisements to a Venue

To apply service advertisements to a venue, follow these steps:

Step 1 Choose **Services > MSAP**.

Step 2 Select the check box of the service advertisement that you to apply to a venue.

Step 3 From the Select a command drop-down list choose **Apply to Venue(s)**.

Step 4 Click **Go**.

Step 5 Follow Step 6 through Step 13 in the Provisioning MSAP Service Advertisements, page 11-98.

or

Click **Apply** to Venues on the MSAP page and follow Step 6 through Step 13 in the Provisioning MSAP Service Advertisements, page 11-98.

Viewing the Configured Service Advertisements

To view the configured service advertisements, follow these steps:

Step 1 Choose **Services > Mobility Services Engine**.

Step 2 Click **Device Name** to view its properties.

The General Properties page appears.

Step 3 Choose **MSAP Service > Advertisements** from the left sidebar menu.

The following information appears in the MSAP Service page:

- Icon—Displays an icon associated with the service provider.
- Provide Name—Displays the service providers name.
- Venue Name—Displays the venue name.
- Advertisements
  - Friendly Name—Friendly name that is displayed in the handset.
  - Advertisement Type—Type of advertisement that is displayed in the handset.

Viewing MSAP Statistics

To view MSAP statistics, follow these steps:

Step 1 Choose **Services > Mobility Services Engine**.

Step 2 Click **Device Name** to view its properties.

The General Properties page appears.

Step 3 Choose **MSAP Service > Statistics** from the left sidebar menu.

The following information appears in the MSAP Service page:

- Top 5 Active Mobile MAC addresses—Displays information of the most active mobiles in a given venue.
- Top 5 Service URIs—Displays information of the usage of the services across a given venue or provider.

Viewing MSE Summary Page for MSAP License Information

See the "Mobility Services Engine (MSE) License Summary" section on page 15-137 for more information on MSE licensing.

Viewing Service Advertisements Synchronization Status

To view service advertisements synchronization status, follow these steps:

Step 1 Choose **Services > Synchronize Services**.

Step 2 Choose **Service Advertisements** from the left side menu bar.

The following information appears in the Service Advertisements page:

- Provider Name—Shows the name of the service provider.
- Service—Shows the type of service that a particular advertisement is using.
- MSE—Shows whether the service advertisement is synchronized with the MSE or not.
- Sync Status—Shows the synchronization status. A green two-arrow icon indicates that its corresponding element is synchronized with the given server such as MSE. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a given server.
- Message—Shows any message related to the advertisement synchronization failure.

Adding an MSAP License Using the License Center

To add an MSAP license using the license center, follow these steps:

Step 1 Choose **Administration > License Center**.

Step 2 Choose **Files > MSE Files** from the left sidebar menu.

The License Center page appears.

Step 3 Click the **Add** to select the license file.

Step 4 Click **OK** to add the license.

The MSAP license is added.

MSAP Reports

You can generate 2 types of MSAP reports:

- Service URI Statistics—In this report, you can retrieve information about the top services that you have used based on the filters like venue, provider, mobile mac and MSAP servers. With this report, you can get the additional information about the usage of the services across a given venue. See the "Service URI Statistics" section on page 14-119 for more information on Service URI Statistics report.
- Mobile MAC Statistics—In this report, you can retrieve information about the most active clients based on the filters like venue and MSAP server. With this report, you can get additional information about the most active mobiles in a given venue. See the "Mobile MAC Statistics" section on page 14-118 for more information on Mobile Mac Statistics.

Identity Services

Cisco Identity Services Engine (ISE) is a next-generation identity and policy-based network access platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations.

NCS manages the wired and the wireless clients in the network. When Cisco ISE is used as a RADIUS server to authenticate clients, NCS collects additional information about these clients from Cisco ISE and provides all relevant client information to NCS to be visible in a single console.

Note NCS communicates with ISE using REST API. See the http://www.cisco.com/en/US/docs/security/ise/1.0/api_ref_guide/ise10_api_ref_guide_ch1.html for more information on Cisco ISE APIs.

Note Accounting data for wired clients are collected from ISE every 15 minutes. There is a background ISE Status task that polls all ISEs added to NCS for every 15 minutes for the status of ISEs and updates the status. See the "Viewing Identity Services Engine Status" section on page 15-19 for more information on viewing identity services engine status.

The ISE integration in NCS provides the following features:

- Periodic polling to ISE for collecting client statistics and other attributes requires for client list, dashboard charts, and reports.
- On demand query to ISE for getting additional client details such as Authorization Profile, Posture, Endpoint Type (profiler), and so on.
- Cross launch ISE user interface with automatic single sign on. See the "Identity Services Engine Reports" section on page 14-129 for more information.

See the "Cisco Identity Service Engine Solution" section on page 1-11 for more information on the ISE integration in NCS.

See the *Cisco Identity Services Engine User Guide, Release 1.0 at the following URL*: http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html for more information about ISE.

This section contains the following topics:

Viewing Identify Services

To see the Identity Services Engines that are added in NCS, choose **Services > Identity Services**. The following parameters appear:

- Server Address—IP address of ISE.
- Port—HTTPS port number for the server.
- Retries—Indicates the number of retry attempts.
- Version—Indicates the version of the ISE.
- Status—Indicates the reachability status, that is, Reachable or Unreachable.
- Role—Indicates if a node is a primary, standalone or, standby node.

Adding an Identity Services Engine

Note A maximum of two ISEs can be added in NCS. If you add two ISEs, one should be primary and the other should be standby. When you are adding a standalone node, you can add only one standalone node and cannot add second node.

To add an Identity Services Engine, follow these steps:

Step 1 Choose **Services > Identity Services**.

Step 2 From the Select a command drop-down list, choose **Add Identity Services Engine**.

Step 3 In the Server Address text box, type the IP address of the server.

Step 4 In the Port text box, enter the port number of the server. The default is 443.

Step 5 In the Username text box, enter the username.

Step 6 In the Password text box, enter the password.

Step 7 Reenter the password in the **Confirm** Password text box.

Note The credentials should be superuser credentials. Otherwise, ISE integration does not work.

Step 8 In the HTTP Connection Timeout text box, enter the amount of time (in seconds) allowed before the process time outs. The default is 30 seconds.

Step 9 Click **Save**.

Removing an Identity Services Engine

To remove an Identity Services Engine, follow these steps:

Step 1 Choose **Services > Identity Services**.

Step 2 Select the check box(es) of the identity services engines that you want to delete.

Step 3 From the Select a command drop-down list, choose **Delete Identity Services Engine(s)**.

Step 4 Click **OK** to confirm the deletion.

CHAPTER 16

Tools

The Tools menu provides access to the Voice Audit, Location Accuracy Tool, Configuration Audit Summary, and Migration Analysis features of the Cisco NCS. This chapter contains the following sections:

Running Voice Audits

The NCS provides voice auditing mechanism to check the controller configuration and to ensure that any deviations from the deployment guidelines are highlighted as an Audit Violation.

To access the Voice Audit feature, choose **Tools > Voice Audit**. The Voice Audit Report page appears.

This page contains three tabs: Controllers, Rules, and Reports.

- The Controllers tab allows you to choose the controller(s) on which to run the voice audit.
- The Rules tab allows you to indicate the applicable VoWLAN SSID and the applicable rules for this voice audit.
- The Report tab provides a summary of the voice audit details and report results.

To access the Voice Audit feature, choose **Tools > Voice Audit**.

This section contains the following topics:

Running Voice Audits on Controllers

The Controllers tab allows you to choose the controller(s) on which to run the voice audit.

Note You can run the voice audit on a maximum of 50 controllers in a single operation.

To select the controller(s) for the voice audit, follow these steps:

Step 1 Choose **Tools > Voice Audit**.

Step 2 Click the **Controllers** tab.

Step 3 From the Run audit on drop-down list, choose **All Controllers**, **A Floor Area**, or **A Single Controller**.

- All Controllers—No additional Controller information is necessary.
- A Floor Area—From the drop-down lists, choose the applicable campus, building, floor, and controller.
- A Single Controller—Choose the applicable controller from the drop-down list.

Step 4 Click the **Rules** tab to determine the rules for this voice audit. See the "Choosing Voice Audit Rules" section on page 16-2 for more information.

Choosing Voice Audit Rules

The Rules tab allows you to indicate the applicable VoWLAN SSID and the applicable rules for this voice audit.

To indicate the rules for the voice audit, follow these steps:

Step 1 In the Tools > Voice Audit page, click the **Rules** tab.

Step 2 Type the applicable VoWLAN SSID in the **VoWLAN SSID** text box.

Step 3 From the **Rules List**, select the check boxes of the applicable rules for this voice audit (see Table 16-1).

Note The red circle indicates an invalid rule (due to insufficient data). The green circle indicates a valid rule.

Table 16-1 Rules List for Voice Audit

Rule	Rule Details
VoWLAN SSID	Description—Checks whether or not the VoWLAN SSID exists. Rule validity—User-defined VoWLAN SSID.
CAC: 7920	Description—Checks whether or not 7920 AP CAC is enabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
CAC: 7920 Clients	Description—Checks whether or not the 7920 Client CAC is disabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.

Table 16-1 Rules List for Voice Audit (continued)

Rule	Rule Details
DHCP Assignment	Description—Checks whether or not DHCP assignment is disabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
MFP Client	Description—Checks whether or not MFP Client protection is not set to **Required** for VoWLAN. Rule validity—User-defined VoWLAN SSID.
Platinum QoS	Description—Checks whether or not QoS is set to Platinum (Voice) for VoWLAN. Rule validity—User-defined VoWLAN SSID.
Non Platinum QoS	Description—Checks that QoS is not set to Platinum for non-VoWLAN. Rule validity—User-defined VoWLAN SSID.
WMM	Description—Checks whether or not WMM is enabled for VoWLAN. Rule data—Choose **Allowed** or **Required** from the drop-down list. Rule validity—User-defined VoWLAN SSID.
CCKM	Description—Checks whether or not CCKM is enabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
CCKM With No AES- for 792x phones	Description—Check that AES encryption is not enabled with Cisco Centralized Key Management (CCKM) for VoWLAN. This rule is only for 792x phones. Rule validity—User-defined VoWLAN SSID.
TSM	Description—Check that Traffic Stream Metrics (TSM) is Enabled. Rule data—Choose **802.11a/n TSM**, **802.11b/g/n TSM**, or both check boxes. Rule validity—At least one band must be selected.
DFS	Description—Checks whether the Channel Announcement and Channel Quite Mode are Enabled for Dynamic Frequency Selection (DFS).
ACM	Description—Checks whether or not Admission Control is enabled. Rule data—Choose **802.11a/n ACM**, **802.11b/g/n ACM**, or both check boxes. Rule validity—At least one band must be selected.
DTPC	Description—Checks whether or not Dynamic Transmit Power Control is enabled. Rule data—Select **802.11a/n DTPC**, **802.11b/g/n DTPC**, or both check boxes. Rule validity—At least one band must be selected.

Table 16-1 Rules List for Voice Audit (continued)

Rule	Rule Details
Expedited Bandwidth	Description—Checks whether or not Expedited Bandwidth is enabled. Rule data—Select **802.11a/n Expedited Bandwidth**, **802.11b/g/n Expedited Bandwidth**, or both check boxes. Rule validity—At least one band must be selected.
Load Based CAC	Description—Checks whether or not Load Based Admission Control (CAC) is enabled. Rule data—Select **802.11a/n Load Based CAC**, **802.11b/g/n Load Based CAC (LBCAC)**, or both check boxes. Rule validity—At least one band must be selected.
CAC: Max Bandwidth	Description—Checks whether or not Maximum RF Bandwidth for Call Admission Control is configured properly. Rule data—Enter percentages in the text boxes for Maximum Allowed Bandwidth for 802.11a/n and 802.11b/g/n. Rule validity—Data for at least one band must be provided. The valid range is 0—100%.
CAC: Reserved Roaming Bandwidth	Description—Checks whether or not Reserved Roaming Bandwidth for Call Admission Control is configured properly. Rule data—Enter percentages in the text boxes for Maximum Reserved Roaming Bandwidth for 802.11a/n and 802.11b/g/n. Rule validity—Data for at least one band must be provided. The valid range is 0—100%.
Pico Cell mode	Description—Checks whether or not Pico Cell mode is disabled. Rule data—Select **802.11a/n Pico Cell mode**, **802.11b/g/n Pico Cell mode**, or both check boxes. Rule validity—At least one band must be selected.
Beacon Period	Description—Checks whether or not Beacon Period is configured properly. Rule data—Enter the time (ms) in the text boxes for Beacon Period for 11a/n and 11b/g/n. Rule validity—Data for at least one band must be provided. The valid range is 20—1000. Enter 0 or keep it empty if a band should not be checked.
Short Preamble	Description—Checks whether or not Short Preamble is enabled for 11b/g.

Table 16-1 Rules List for Voice Audit (continued)

Rule	Rule Details
Fragmentation Threshold	Description—Checks whether or not Fragmentation Threshold is configured properly. Rule data—Enter the threshold amount (bytes) in the text boxes for Fragmentation Threshold for 11a/n and 11b/g/n. Rule validity—Data for at least one band must be provided. The valid range is 256—2346. Enter 0 or keep it empty if a band should not be checked.
Data Rate	Description—Checks whether or not Data Rates are configured properly. Data Rate configuration for 11b/g—Select **Disabled**, **Supported**, or **Mandatory** for each Mbps category. Data Rate configuration for 11a—Select **Disabled**, **Supported**, or **Mandatory** for each Mbps category.
Aggressive Load Balancing	Description—Checks whether or not Aggressive Load Balancing is disable.
QoS Profile	Description—Checks that QoS Profiles are not altered from default values.
EAP Request Timeout	Description—Checks whether or not EAP Request Timeout is configured properly. Rule data—Enter the time limit (sec) for the EAP Request Timeout. Rule validity—Data cannot be left blank or as zero. The valid range is 1—120.
ARP Unicast	Description—Checks whether or not ARP Unicast is disabled.

Note Click **Reset** to reset the rules to the default configuration.

Step 4 When the rules are configured for this voice audit, click **Save** to save the current configuration or **Save and Run** to save the configuration and run the report.

Step 5 Click the **Report** tab to view the Report results. See the "Voice Audit Report Details" section on page 16-5 for more information.

Voice Audit Report Details

The Voice Audit details provides the following information:

- Audit Status—Indicates whether or not the audit is complete.
- Start Time and End Times—Indicates the time at which the voice audit starts and ends.
- # Total Devices—Indicates the number of devices involved in the voice audit.
- # Completed Devices—Indicates the number of devices the tool attempted to audit.

Note If a controller is unreachable, the audit skips it. The Voice Audit does not complete any rule checks for that controller.

- # Rules—Indicates the number of rules selected for the voice audit.

Voice Audit Report Results

The Voice Audit Report results include the following information:

- IP Address—Indicates the IP address for the controller involved in the voice audit.
- Rule—Indicates the rule that was applied for this controller.
- Result—Indicates the result (Skipped, Violation, Unreachable) of the applied rule.

Note If there is no mismatch between the current configuration and a rule value, no results are displayed for that rule.

- Details—Defines an explanation for the rule results.

Note If the applied rule results in a Violation, the Details link provides additional information including Name, the Device Value, and the Rule Value. Hover your mouse cursor over the link to view the additional details.

- Time—Provides a timestamp for the voice audit.

Configuring the Location Accuracy Tools

You can analyze the location accuracy of non-rogue and rogue clients, interferers, and asset tags by using the Location Accuracy Tools.

By verifying for location accuracy, you are ensuring that the existing access point deployment can estimate the true location of an element within 10 meters at least 90% of the time.

The Location Accuracy Tools enable you to run either of the following tests:

There are two ways to test location accuracy:

- **Scheduled Accuracy Testing**—Employed when clients, tags, and interferers are already deployed and associated to the wireless LAN infrastructure. Scheduled tests can be configured and saved when clients, tags, and interferers are already pre-positioned so that the test can be run on a regularly scheduled basis.
- **On-Demand Accuracy Testing**—Employed when elements are associated but not pre-positioned. On-demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy for a small number of clients, tags, and interferers.

Both are configured and executed through a single page.

This section contains the following topics:

- Enabling the Location Accuracy Tool, page 16-7

Enabling the Location Accuracy Tool

Note You must enable the **Advanced Debug** option in the NCS to use the Scheduled and On-demand location accuracy tool testing features. The Location Accuracy Tool does not appear as an option on the Tools menu when the Advanced Debug option is not enabled.

To enable the advanced debug option in the NCS, follow these steps:

Step 1 In the NCS, choose **Monitor > Maps**.

Step 2 Choose **Properties** from the Select a command drop-down list, and click **Go**.

Step 3 In the page that appears, select the **Enabled** check box to enable the Advanced Debug Mode. Click **OK**.

Note If Advanced Debug is already enabled, you do not need to do anything further. Click **Cancel**.

You can now run location accuracy tests on the mobility services engine using the Location Accuracy Tool.

Proceed to either the "Using Scheduled Accuracy Testing to Verify Accuracy of Current Location" section on page 16-8 or "Using On-demand Accuracy Testing to Test Location Accuracy" section on page 16-10.

Viewing Currently Scheduled Accuracy Tests

To view the currently scheduled location accuracy tests, follow these steps:

Step 1 Select **Tools > Location Accuracy Tool**.

Step 2 The Accuracy Tests page displays all currently scheduled accuracy tests. The page displays the following information:

- Test Name—Click the Name to view details regarding this accuracy test.
- Test Type
- Floor or Outdoor Area—Displays the location of this test.
- Status
- Accuracy %
- Average Errors (m)

Use the Select a command drop-down list to create a new scheduled or on-demand accuracy test, to download logs for last run, to download all logs, or to delete a current accuracy test.

Note

- You can download logs for accuracy tests from the Accuracy Tests summary page. To do so, select an accuracy test and from the Select a command drop-down list, choose either **Download Logs** or **Download Logs for Last Run**. Click **Go**.
- The Download Logs option downloads the logs for all accuracy tests for the selected test(s).
- The Download Logs for Last Run option downloads logs for only the most recent test run for the selected test(s).

Viewing Accuracy Test Details

To view details regarding a current accuracy test, follow these steps:

Step 1 Choose **Tools > Location Accuracy Tool**.

Step 2 Click the name of the accuracy test for which you want to access details.

In the Accuracy Test Details page, you can position test points or delete the accuracy test.

Step 3 Click **Cancel** to return to the Accuracy Test overview page.

Using Scheduled Accuracy Testing to Verify Accuracy of Current Location

To configure a scheduled accuracy test, follow these steps:

Step 1 Choose **Tools > Location Accuracy Tool**.

Step 2 Choose **New Scheduled Accuracy Test** from the Select a command drop-down list.

Step 3 Enter a Test Name.

Step 4 Choose the **Area Type** from the drop-down list.

Step 5 Campus is configured as Root Area, by default. There is no need to change this setting.

Step 6 Choose the Building from the drop-down list.

Step 7 Choose the Floor from the drop-down list.

Step 8 Choose the begin and end time of the test by entering the days, hours, and minutes. Hours are entered using a 24-hour clock.

Note When entering the test start time, be sure to allow enough time prior to the test start to position testpoints on the map.

Step 9 Test results are viewed in the Accuracy Tests > Results page. Reports are in PDF format.

Note If you choose the e-mail option, an SMTP Mail Server must first be defined for the target e-mail address. Choose **Administrator > Settings > Mail Server** to enter the appropriate information.

Step 10 Click **Position Testpoints**. The floor map appears with a list of all clients, tags, and interferers on that floor with their MAC addresses.

Step 11 Select the check box next to each client, tag, and interferer for which you want to check the location accuracy.

When you select a MAC address check box, two icons appear on the map. One icon represents the actual location and the other represents the reported location.

Note To enter a MAC address for a client or tag or interferer that is not listed, select the **Add New MAC** check box, enter the MAC address, and click **Go**. An icon for the element appears on the map. If the newly added element is on the location server but on a different floor, the icon is displayed in the left-most corner (0,0 position).

Step 12 If the actual location for an element is not the same as the reported location, drag the actual location icon for that element to the correct position on the map. Only the actual location icon can be dragged.

Step 13 Click **Save** when all elements are positioned. A dialog box appears confirming successful accuracy testing.

Step 14 Click **OK** to close the confirmation dialog box. You are returned to the Accuracy Tests summary page.

Note The accuracy test status is displayed as Scheduled when the test is about to execute. A status of Running is displayed when the test is in process and Idle when the test is complete. A Failure status appears when the test is not successful.

Step 15 To view the results of the location accuracy test, click the test name and then click the **Results** tab in the page that appears.

Step 16 In the Results page, click the **Download** link under the Saved Report heading to view the report.

The Scheduled Location Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram.
- A cumulative error distribution graph.
- An error distance over time graph.
- A summary by each MAC address whose location accuracy was tested noting its actual location, error distance and a map showing its spatial accuracy (actual vs. calculated location), and error distance over time for each MAC.

Using On-demand Accuracy Testing to Test Location Accuracy

An On demand Accuracy Test is run when elements are associated but not pre-positioned. On demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy for a small number of clients, tags, and interferers.

To run an On-demand Accuracy Test, follow these steps:

Step 1 Choose **Tools > Location Accuracy Tool**.

Step 2 From the Select a command drop-down list, choose **New On demand Accuracy Test**.

Step 3 Enter a Test Name.

Step 4 Choose **Area Type** from the drop-down list.

Step 5 Campus is configured as Root Area, by default. There is no need to change this setting.

Step 6 Choose the Building from the drop-down list.

Step 7 Choose the Floor from the drop-down list.

Step 8 Choose the Destination point for the test results. Test results are viewed in the Accuracy Tests > Results page. Reports are in PDF format.

Step 9 Click **Position Testpoints**. The floor map appears with a red crosshair at the (0,0) coordinate.

Step 10 To test the location accuracy and RSSI of a particular location, select either client or tag or interferer from the drop-down list on the left. A list of all MAC addresses for the selected option (client or tag or interferer) displays in a drop-down list to its right.

Step 11 Choose a MAC address from the drop-down list, move the red cross hair to a map location, and click the mouse to place it.

Step 12 From the Zoom percentage drop-down list, choose the zoom percentage for the map.

The X and Y text boxes are populated with the coordinates based on the position of the red cross hair in the map.

Step 13 Click **Start** to begin collection of accuracy data.

Step 14 Click **Stop** to finish collection. You should allow the test to run for at least two minutes before clicking Stop.

Step 15 Repeat Step 11 to Step 14 for each testpoint that you want to plot on the map.

Step 16 Click **Analyze Results** when you are finished mapping the testpoints.

Step 17 Click the **Results** tab in the page that appears.

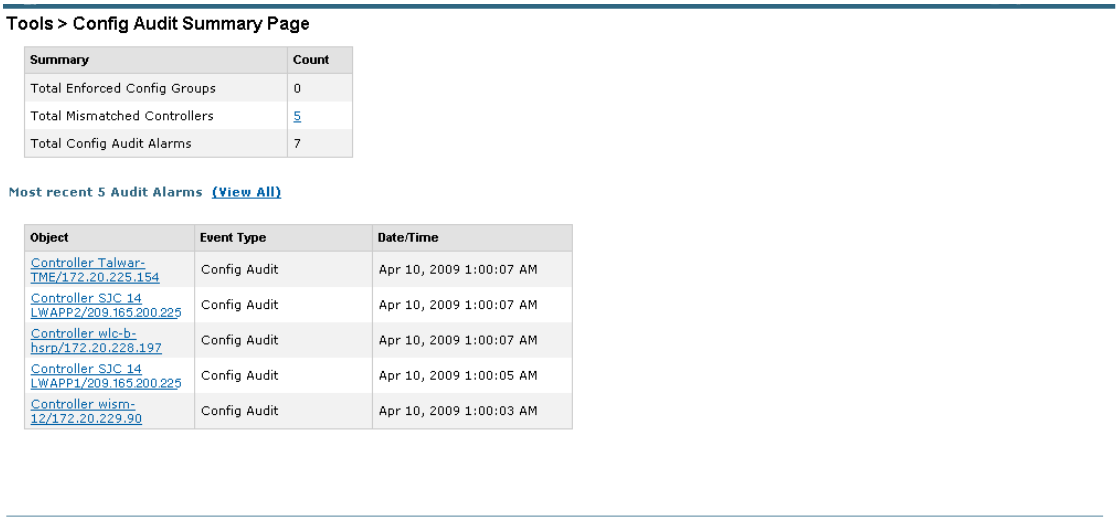
The On-demand Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram
- A cumulative error distribution graph

Configuring Audit Summary

Choose **Tools > Config Audit** to launch the Config Audit Summary page (see Figure 16-1).

Figure 16-1 Tools > Config Audit Summary Page



This page provides a summary of the following:

- Total Enforced Config Groups—Identifies the count of config group templates, which are configured for Background Audit and are enforcement enabled.

  Click the link to launch the Config Group page to view config groups with Enforce Configuration enabled.

- Total Mismatched Controllers—Identifies the number of mismatched controllers. Mismatched controllers indicate that there were configuration differences found between the NCS and the controller during the last audit.

  Click the link to launch the controller list sorted in the mismatched audit status column. Click an item in the Audit Status column to view the audit report for this controller.

- Total Config Audit Alarms—Identifies the number of alarms generated when audit discrepancies are enforced on config groups.

  Click the link to view all config audit alarm details.

  Note If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group. The alarms have links to the audit report where you can view a list of discrepancies for each controller.

- Most recent 5 config audit alarms—Lists the most recent configuration audit alarms including the object name, event type, date, and time for the audit alarm.

Click **View All** to view the applicable Alarm page that includes all configuration audit alarms.

Configuring Migration Analysis

Choose **Tools > Migration Analysis** to launch the Migration Analysis Summary page.

Note You can also access the migration analysis summary by choosing **Configure > Autonomous AP > Migration Templates** and choosing **View Migration Analysis Summary** from the Select a command drop-down list.

The autonomous access points are eligible for migration only if all the criteria has a pass status. A red X designates ineligibility, and a green check mark designates eligibility. These columns represent the following:

- Privilege 15 Criteria—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.
- Software Version—Conversion is supported only from 12.3(7)JA releases excluding 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, and 12.3(11)JA3.
- Role Criteria—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
  - root
  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only

Radio Criteria—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.

This section contains the following topics:

- Upgrading Autonomous Access Points, page 16-12
- Viewing a Firmware Upgrade Report, page 16-13
- Viewing a Role Change Report, page 16-14

Upgrading Autonomous Access Points

You can choose to upgrade the autonomous access points manually or automatically. In the Migration Analysis page, you can select the access point with the software version listed as failed and choose **Upgrade Firmware (Manual or Automatic)** from the Select a command drop-down list. This process upgrades the autonomous firmware image of the Cisco IOS access point to a supported version.

The NCS uses a Telnet-based connection to upgrade the access point firmware. If you choose the automatic option, the internal TFTP server is used with the default images present in the NCS. The default images per device type are as follows:

- ap801-k9w7-tar.124-10b.JA3.tar
- ap802-k9w7-tar
- c1100-k9w7-tar.123-7.JA5.tar
- c1130-k9w7-tar.123-7.JA5.tar

- c1200-k9w7-tar.123-7.JA5.tar
- c1240-k9w7-tar.12307.JA5.tar
- c1250-k9w7-tar.124-10b.JA3.tar
- c1310-k9w7-tar.123-7.JA5.tar

If you choose the manual option, an additional page with TFTP server IP, file path, and file pathname appears. The final page is the Report page.

Changing Station Role to Root Mode

Because a wired connection between the access point and controller is required to send the association request, the autonomous access point must be assigned the appropriate role. If the role shows as ineligible, choose **Change Station Role to Root Mode** from the Select a command drop-down list to change the mode.

Running Migration Analysis

Choose **Run Migration Analysis** from the Select a command drop-down list of the Migration Analysis Summary page. The resulting migration analysis summary shows the current status of different criteria. Initially, migration analysis is run automatically when the access point is discovered.

Viewing the Migration Analysis Report

You can choose **View Migration Analysis Report** from the Select a command drop-down list of the Migration Analysis Summary page to generate a report. The report includes the following:

- Access point address
- Status
- Timestamp
- Access point logs

Viewing a Firmware Upgrade Report

Choose **View Firmware Upgrade Report** from the Select a command drop-down list to view a current report of the upgrade status for the selected access point.

The following information is displayed:

- AP Address—IP address of the access point.
- Status—Current status of the firmware upgrade.
- TimeStamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

See the "Upgrading Autonomous Access Points" section on page 16-12 for more information.

Viewing a Role Change Report

Because a wired connection between the access point and controller is required to send the association request, the autonomous access point must be assigned the appropriate role.

To view a report of these role changes, choose **View Role Change Report** from the Select a command drop-down list. The following information is displayed:

- AP Address—IP address of the access point.
- Status—Current status of the role change.
- TimeStamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

Configuring TAC Case Attachments

Note You must configure a valid mail server before configuring TAC case attachments.

The TAC Case Attachment tool helps you easily attach all the relevant controller TAC case information in one step. This tool provides two options:

- Send—Sends an e-mail to attach@cisco.com.
- Download—Downloads the information to a local computer. You must manually e-mail the data to attach@cisco.com. This option is handy if there is no e-mail connectivity between the NCS server and Cisco or if the information is too large to be attached through e-mail.

This tool sends the following information:

- Network Information—Sends device inventory details and the client types.
- Controller Information—Sends running configuration details, tech-support, message logs, trap logs, and the controller crash files.
- Access Point Information—Sends crash files and radio core dumps.

To Send or Download information, you must enter the following details:

- Enter a valid TAC Case Number.
- Select a controller if you want to send the controller or AP information.

Note You can also send additional information using the additional comments text box. After sending the information, you can verify whether the data has reached Cisco by looking at the attachment section in the Case tool.

Note This tool requires read-write access on the controller to collect and upload controller or access point information.

CHAPTER 17

wIPS Policy Alarm Encyclopedia

Security IDS/IPS Overview

The addition of WLANs in the corporate environment introduces a new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured and unconfigured access points and DoS (denial of service) attacks.

The Cisco Adaptive Wireless IPS is designed to help manage against security threats by validating proper security configurations and detecting possible intrusions. With the comprehensive suite of security monitoring technologies, the Cisco Adaptive Wireless IPS alerts the user on more than 100 different threat conditions in the following categories:

- User authentication and traffic encryption
- Rogue and ad-hoc mode devices
- Configuration vulnerabilities
- Intrusion detection on security penetration
- Intrusion detection on DoS attacks

To maximize the power of the Cisco Adaptive Wireless IPS, security alarms can be customized to best match your security deployment policy. For example, if your WLAN deployment includes access points made by a specific vendor, the product can be customized to generate the rogue access point alarm when an access point made by another vendor is detected by the access point or sensor.

Note The wIPS Local Mode or FlexConnect Mode access points do not support all security alarms. The magnifying glass icon indicates that this alarm is not supported by the wIPS Local Mode or FlexConnect Mode access points.

Pre-configured Profiles for Various WLAN Environments

During installation, the user can select an appropriate profile based on the WLAN network implemented.

The Cisco Adaptive Wireless IPS provides separate profiles for the following:

- Enterprise best practice
- Enterprise rogue detection only

- Financial (Gramm-Leach-Bliley Act compliant)
- HealthCare (Health Insurance Portability and Accountability Act compliant)
- Hotspot implementing 802.1x security
- Hotspot implementing NO security
- Tradeshow environment
- Warehouse/manufacturing environment
- Government/Military (8100.2 directive compliant)
- Retail environment

When the administrator selects the appropriate profile, the Cisco Adaptive Wireless IPS enables or disables alarms from the policy profile that are appropriate for that WLAN environment. For example, health care institutions can select the Healthcare profile and all alarms that are necessary to be HIPAA compliant are enabled. The administrator still has the option after installation to enable or disable any alarm or change the threshold values as per individual preferences.

The Cisco Adaptive Wireless IPS system not only is an IDS (Intrusion Detection System), but also is an IPS (Intrusion Prevention System).

Tip To learn more about Cisco Adaptive wIPS features and functionality, go to Cisco.com to watch a multimedia presentation. Here you also find the learning modules for a variety of NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

Cisco Adaptive Wireless IPS policies are included in two security subcategories: wIPS—Denial of Service (DoS) Attacks and wIPS—Security Penetration.

This section contains the following topics:

Intrusion Detection—Denial of Service Attack

Wireless DoS (denial of service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLANs at layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example, RF jamming attacks with a high-power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

The nature and protocol standards for wireless are subject to some of these attacks. Cisco has developed Management Frame Protection, the basis of 802.11i, to proactively prevent many of these attacks. (For more information on MFP, see the Cisco NCS online help.) The Cisco Adaptive Wireless IPS contributes to this solution by an early detection system where the attack signatures are matched. The Cisco Adaptive Wireless IPS DoS detection focuses on WLAN layer one (physical layer) and two (data link layer, 802.11, 802.1x). When strong WLAN authentication and encryption mechanisms are used, higher layer (IP layer and above) DoS attacks are difficult to execute. The wIPS server tightens your WLAN defense by validating strong authentication and encryption policies. In addition, the Cisco Adaptive Wireless IPS Intrusion Detection on denial of service attacks and security penetration provides 24 X 7 air tight monitoring on potential wireless attacks.

This section describes the denial of service attack subcategories and contains the following topics:

Denial of Service Attack Against Access Points

DoS attacks against access points are typically carried out on the basis of the following assumptions:

- Access points have limited resources. For example, the per-client association state table.
- WLAN management frames and authentication protocols 802.11 and 802.1x have no encryption mechanisms.

Wireless intruders can exhaust access point resources, most importantly the client association table, by emulating large number of wireless clients with spoofed MAC addresses. Each one of these emulated clients attempts association and authentication with the target access point but leaves the protocol transaction mid-way. When the access point resources and the client association table is filled up with these emulated clients and their incomplete authentication states, legitimate clients can no longer be serviced by the attacked access point. This creates a denial of service attack.

The Cisco Adaptive Wireless IPS tracks the client authentication process and identifies DoS attack signatures against the access point. Incomplete authentication and association transactions trigger the attack detection and statistical signature matching process. Detected DoS attacks result in setting off wIPS alarms which include the usual alarm detail description and target device information.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing.

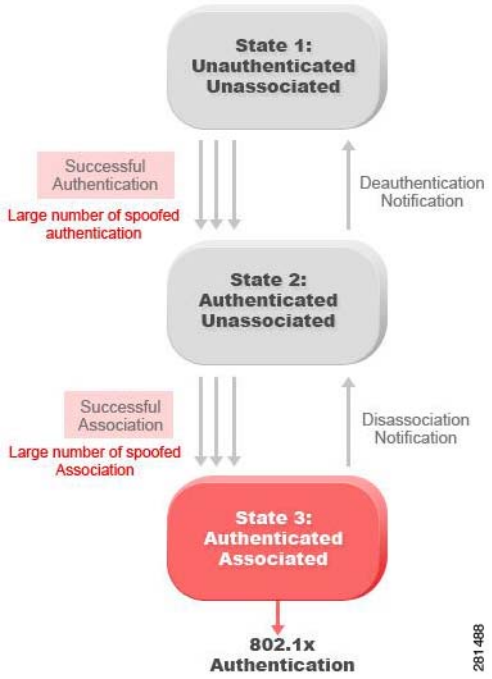
This section describes the DoS attacks against access points and contains the following topics:

Denial of Service Attack: Association Flood

Alarm Description and Possible Causes

This DoS attack exhausts the access point resources, particularly the client association table, by flooding the access point with a large number of spoofed client associations. At the 802.11 layer, shared-key authentication is flawed and rarely used. The other alternative is open authentication (null authentication) that relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker using such a vulnerability can emulate a large number of clients to flood a target access point client association table by creating many clients reaching State 3. When the client association table overflows, legitimate clients cannot get associated; therefore, a DoS attack is committed. (See Figure 17-1)

Figure 17-1 DoS Attack: Association Flood



wIPS Solution

The Cisco Adaptive Wireless IPS detects spoofed MAC addresses and tracks the 802.1x actions and data communication after a successful client association to detect this form of DoS attack. After this attack is reported by the Cisco Adaptive Wireless IPS, you may log onto this access point to inspect its association table for the number of client associations.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing.

Denial of Service Attack: Association Table Overflow

Alarm Description and Possible Causes

Wireless intruders can exhaust access point resources, most importantly the client association table, by imitating a large number of wireless clients with spoofed MAC addresses. Each one of these imitated clients attempts association and authentication with the target access point. The 802.11 authentication typically completes because most deployments use 802.11 open system authentication, which is a null authentication process. Association with these imitated clients follows the authentication process. These imitated clients do not, however, follow up with higher level authentication such as 802.1x or VPN, which leaves the protocol transaction half-finished. At this point, the attacked access point maintains a state in the client association table for each imitated client. When the access point resources and client association table is filled with these imitated clients and their state information, legitimate clients can no longer be serviced by the attacked access point. This creates a DoS attack.

wIPS Solution

The Cisco Adaptive Wireless IPS tracks the client authentication process and identifies a DoS attack signature against an access point. Incomplete authentication and association transactions trigger the Cisco Adaptive Wireless IPS attack detection and statistical signature matching process.

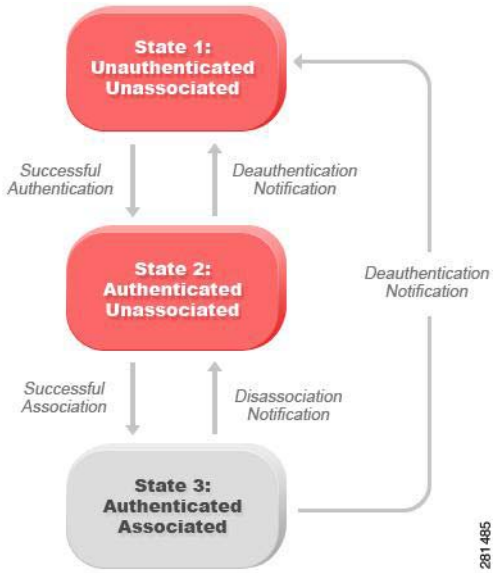
Denial of Service Attack: Authentication Flood

Attack tool: Void11

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement such a state machine according to the IEEE standard (see Figure 17-2). On the access point, each client has a state recorded in the access point client table (association table). This recorded state has a size limit that can either be a hard-coded number or a number based on the physical memory constraint.

Figure 17-2 Client State Machine



A form of DoS attack floods the access point client state table (association table) by imitating many client stations (MAC address spoofing) sending authentication requests to the access point. Upon receipt of each individual authentication request, the target access point creates a client entry in State 1 of the association table. If open system authentication is used for the access point, the access point returns an *authentication success* frame and moves the client to State 2. If shared-key authentication is used for the access point, the access point sends an *authentication challenge* to the attacker imitated client, which does not respond. In this case, the access point keeps the client in State 1. In either case, the access point contains multiple clients hanging in either State 1 or State 2 which fills up the access point association table. When the table reaches its limit, legitimate clients cannot authenticate and associate with this access point. This results in a DoS attack.

wIPS Solution

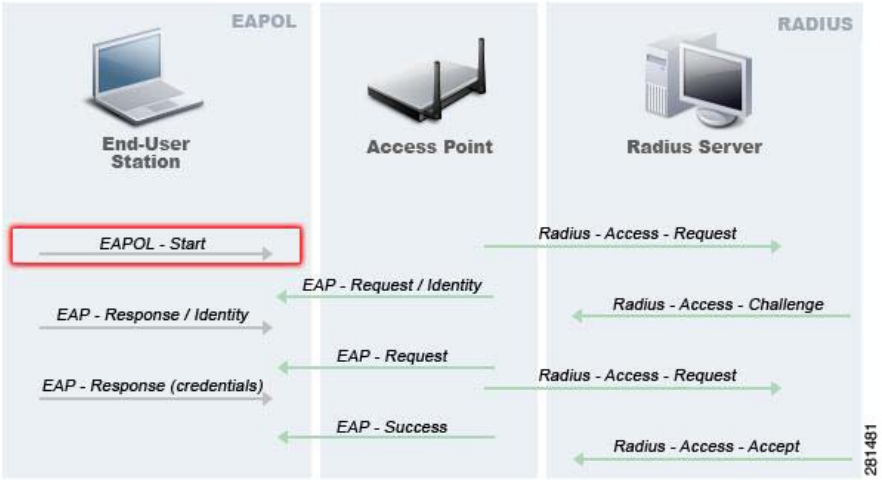
The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security analyst can log onto the access point to check the current association table status.

Denial of Service Attack: EAPOL-Start Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP over LANs (EAPOL). The 802.1x protocol starts with an EAPOL-Start frame sent by the client station to begin the authentication transaction. The access point responds to an EAPOL-start frame with a EAP-identity-request and some internal resource allocation.

Figure 17-3 EAPOL-Start Protocol and EAPOL-Start Attack



An attacker attempts to disrupt an access point by flooding it with EAPOL-start frames to exhaust the access point internal resources.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking the 802.1x authentication state transition and particular attack signature.

Denial of Service Attack: PS Poll Flood

Alarm Description and Possible Causes

Power management is probably one of the most critical features of wireless LAN devices. Power management helps to conserve power by enabling stations to remain in power saving state mode for longer periods of time and to receive data from the access point only at specified intervals.

The wireless client device must inform the access point of the length of time that it is in the sleep mode (power save mode). At the end of the time period, the client wakes up and checks for waiting data frames. After it completes a handshake with the access point, it receives the data frames. The beacons from the access point also include the Delivery Traffic Indication Map (DTIM) to inform the client when it needs to wake up to accept multicast traffic.

The access point continues to buffer data frames for the sleeping wireless clients. Using the Traffic Indication Map (TIM), the access point notifies the wireless client that it has buffered data buffered. Multicast frames are sent after the beacon that announces the DTIM.

The client requests the delivery of the buffered frames using PS-Poll frames to the access point. For every PS-Poll frame, the access point responds with a data frame. If there are more frames buffered for the wireless client, the access point sets the data bit in the frame response. The client then sends another PS-Poll frame to get the next data frame. This process continues until all the buffered data frames are received.

A potential hacker could spoof the MAC address of the wireless client and send out a flood of PS-Poll frames. The access point then sends out the buffered data frames to the wireless client. In reality, the client could be in the power safe mode and would miss the data frames.

wIPS Solution

The Cisco Adaptive Wireless IPS can detect this DoS attack that can cause the wireless client to lose legitimate data. Locate and remove the device from the wireless environment.

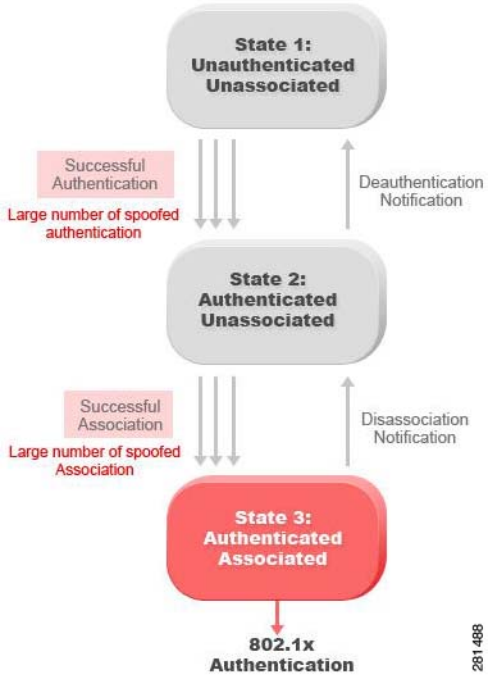
Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing.

Denial of Service Attack: Unauthenticated Association

Alarm Description and Possible Causes

A form of DoS attack is to exhaust the access point resources, particularly the client association table, by flooding the access point with a large number of spoofed client associations. At the 802.11 layer, shared-key authentication is flawed and rarely used. The other alternative is open authentication (null authentication) which relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker using such a vulnerability can imitate a large number of clients to flood a target access point client association table by creating many clients reaching State 3. When the client association table overflows, legitimate clients cannot get associated causing a DoS attack.

Figure 17-4 DoS Attack: Unauthenticated Association



wIPS Solution

The Cisco Adaptive Wireless IPS detects spoofed MAC addresses and tracks 802.1x actions and data communication after a successful client association to detect this form of DoS attack. After this attack is reported by the Cisco Adaptive Wireless IPS, you may log onto this access point to inspect its association table for the number of client associations.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing.

Denial of Service Attack Against Infrastructure

In addition to attacking access points or client stations, the wireless intruder may target the RF spectrum or the back-end authentication RADIUS server for DoS attacks. The RF spectrum can be easily disrupted by injecting RF noise generated by a high power antenna from a distance. Back-end RADIUS servers can be overloaded by a DDoS (distributed denial of service) attack where multiple wireless attackers flood the RADIUS server with authentication requests. This attack does not require a successful authentication to perform the attack.

This section describes the DoS attacks against infrastructure and contains the following topics:

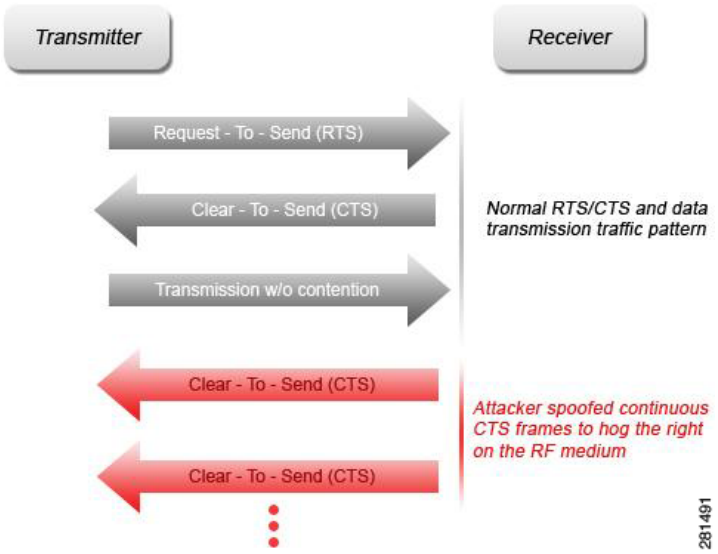
Denial of Service Attack: CTS Flood

Attack tool: CTS Jack

Alarm Description and Possible Causes

As an optional feature, the IEEE 802.11 standard includes the RTS/CTS (request-to-send/clear-to-send) functionality to control the station access to the RF medium. The wireless device ready for transmission sends a RTS frame to acquire the right to the RF medium for a specified time duration. The receiver grants the right to the RF medium to the transmitter by sending a CTS frame of the same time duration. All wireless devices observing the CTS frame should yield the media to the transmitter for transmission without contention.

Figure 17-5 Standard RTS/CTS Functionality Compared to the CTS DoS Attack



A wireless DoS attacker may take advantage of the privilege granted to the CTS frame to reserve the RF medium for transmission. By transmitting back-to-back CTS frames, an attacker can force other wireless devices sharing the RF medium to hold back their transmission until the attacker stops transmitting the CTS frames.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the abuse of CTS frames for a DoS attack.

Denial of Service Attack: Queensland University of Technology Exploit

Denial of Service Vulnerability in IEEE 802.11 Wireless Devices: US-CERT VU#106678 & Aus-CERT AA-2004.02.

Alarm Description and Possible Causes

802.11 WLAN devices use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the basic access mechanism in which the WLAN device listens to the medium before starting any transmission and backs-off when it detects any existing transmission taking place. Collision avoidance combines the physical sensing mechanism and the virtual sense mechanism that includes the Network Allocation Vector (NAV), the time before which the medium is available for transmission. Clear Channel Assessment (CCA) in the DSSS protocol determines whether a WLAN channel is clear so an 802.11b device can transmit on it.

Mark Looi, Christian Wullems, Kevin Tham and Jason Smith from the Information Security Research Centre, Queensland University of Technology, Brisbane, Australia, have recently discovered a flaw in the 802.11b protocol standard that could potentially make it vulnerable to DoS radio frequency jamming attacks.

This attack specifically attacks the CCA functionality. According to the AusCERT bulletin, "an attack against this vulnerability exploits the CCA function at the physical layer and causes all WLAN nodes within range, both clients and access points, to defer transmission of data for the duration of the attack. When under attack, the device behaves as if the channel is always busy, preventing the transmission of any data over the wireless network."

This DoS attack affects DSSS WLAN devices including IEEE 802.11, 802.11b, and low-speed (below 20 Mbps) 802.11g wireless devices. IEEE 802.11a (using OFDM), high-speed (above 20 Mbps using OFDM) 802.11g wireless devices are not affected by this attack. Devices that use FHSS are also not affected.

Any attacker using a PDA or a laptop equipped with a WLAN card can launch this attack on SOHO and enterprise WLANs. Switching to the 802.11a protocol is the only solution or known protection against this DoS attack.

For more information on this DoS attack, refer to:

- www.isrc.qut.edu.au
- www.isrc.qut.edu.au/wireless
- http://www.auscert.org.au/render.html?it=4091
- http://www.kb.cert.org/vuls/id/106678

wIPS Solution

The Cisco Adaptive Wireless IPS detects this DoS attack and sets off the alarm. Locate and remove the responsible device from the wireless environment.

Denial of Service attack: RF Jamming

Alarm Description and Possible Causes

WLAN reliability and efficiency depend on the quality of the radio frequency (RF) media. Each RF is susceptible to RF noise impact. An attacker using this WLAN vulnerability can perform two types of DoS attacks:

- Disrupt WLAN service—At the 2.4 GHz unlicensed spectrum, the attack may be unintentional. A cordless phone, Bluetooth devices, microwave, wireless surveillance video camera, or baby monitor can all emit RF energy to disrupt WLAN service. Malicious attacks can manipulate the RF power at 2.4 GHz or 5 GHz spectrum with a high-gain directional antenna to amplify the attack impact from a distance. With free-space and indoor attenuation, a 1-kW jammer 300 feet away from a building

can jam 50 to 100 feet into the office area. The same 1-kW jammer located inside a building can jam 180 feet into the office area. During the attack, WLAN devices in the target area are out of wireless service.

- Physically damage AP hardware—An attacker using a high-output transmitter with directional high gain antenna 30 yards away from an access point can pulse enough RF power to damage electronics in the access point putting it being permanently out of service. Such High Energy RF (HERF) guns are effective and are inexpensive to build.

wIPS Solution

The Cisco Adaptive Wireless IPS detects continuous RF noise over a certain threshold for a potential RF jamming attack.

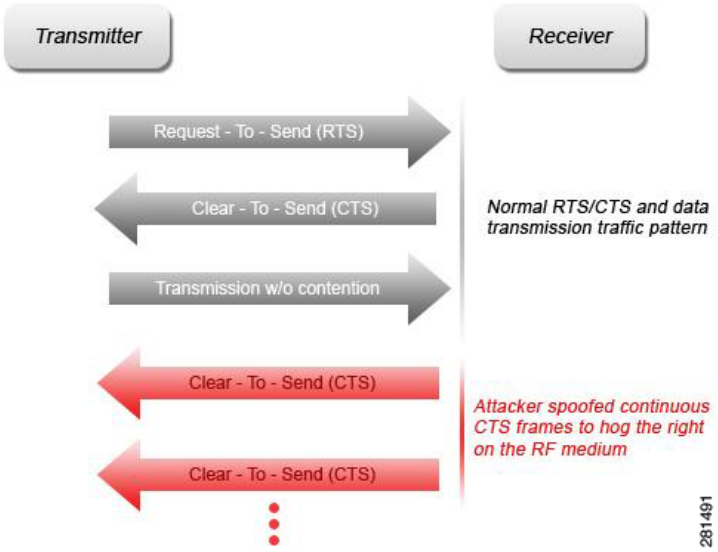
Cisco Spectrum Intelligence also provides specific detection of non-802.11 jamming devices. For more information on Cisco Spectrum Intelligence, refer to the *Cisco Wireless Control System Configuration Guide*.

Denial of Service: RTS Flood

Alarm Description and Possible Causes

As an optional feature, the IEEE 802.11 standard includes the RTS/CTS (Request-To-Send/Clear-To-Send) functionality to control access to the RF medium by stations. The wireless device ready for transmission sends an RTS frame to acquire the right to the RF medium for a specified duration. The receiver grants the right to the RF medium to the transmitter by sending a CTS frame of the same duration. All wireless devices observing the CTS frame should yield the RF medium to the transmitter for transmission without contention. See Figure 17-6.

Figure 17-6 Standard RTS/CTS mechanism vs. intruder-injected RTS DoS attack



A wireless denial of service attacker may take advantage of the privilege granted to the CTS frame to reserve the RF medium for transmission. By transmitting back-to-back RTS frames with a large transmission duration field, an attacker reserves the wireless medium and force other wireless devices sharing the RF medium to hold back their transmissions.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the abuse of RTS frames for denial of service attacks.

Denial of Service Attack: Virtual Carrier Attack

Alarm Description and Possible Causes

The virtual carrier-sense attack is implemented by modifying the 802.11 MAC layer implementation to allow random duration values to be sent periodically. This attack can be carried out on the ACK, data, RTS, and CTS frame types by using large duration values. By doing this the attacker can prevent channel access to legitimate users.

Under normal circumstances, the only time a ACK frame carries a large duration value is when the ACK is part of a fragmented packet sequence. A data frame legitimately carries a large duration value only when it is a subframe in a fragmented packet exchange.

One approach to deal with this attack is to place a limit on the duration values accepted by nodes. Any packet containing a larger duration value is truncated to the maximum allowed value. Low cap and high cap values can be used. The low cap has a value equal to the amount of time required to send an ACK frame, plus media access backoffs for that frame. The low cap is used when the only packet that can follow the observed packet is an ACK or CTS. This includes RTS and all management (association, and so on) frames. The high cap is used when it is valid for a data packet to follow the observed frame. The

limit in this case needs to include the time required to send the largest data frame, plus the media access backoffs for that frame. The high cap must be used in two places: when observing an ACK (because the ACK my be part of a MAC level fragmented packet) and when observing a CTS.

A station that receives an RTS frame also receives the data frame. The IEEE 802.11 standard specifies the exact times for the subsequent CTS and data frames. The duration value of RTS is respected until the following data frame is received or not received. Either the observed CTS is unsolicited or the observing node is a hidden terminal. If this CTS is addressed to a valid in-range station, the valid station can nullify this by sending a zero duration null function frame. If this CTS is addressed to an out-of-range station, one method of defense is to introduce authenticated CTS frames containing cryptographically signed copies of the preceding RTS. With this method, there is a possibility of overhead and feasibility issues.

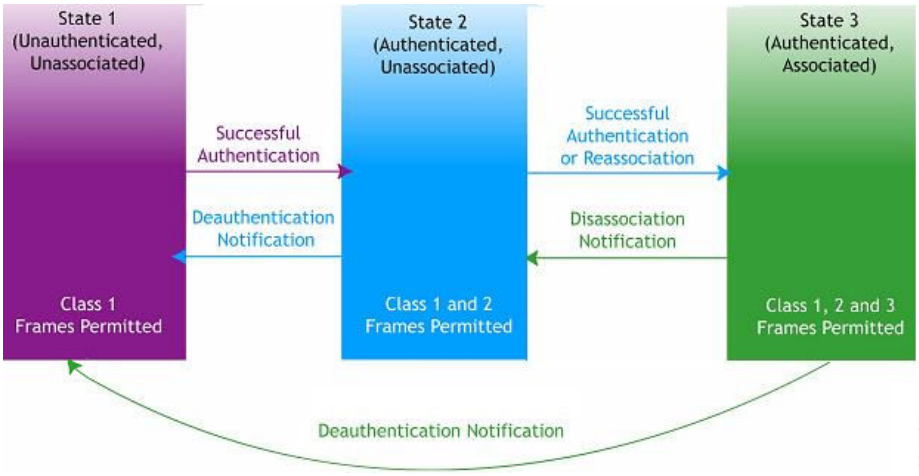
wIPS Solution

The Cisco Adaptive Wireless IPS detects this DoS attack. Locate the device and take appropriate steps to remove it from the wireless environment.

Denial of Service Attack Against Client Station

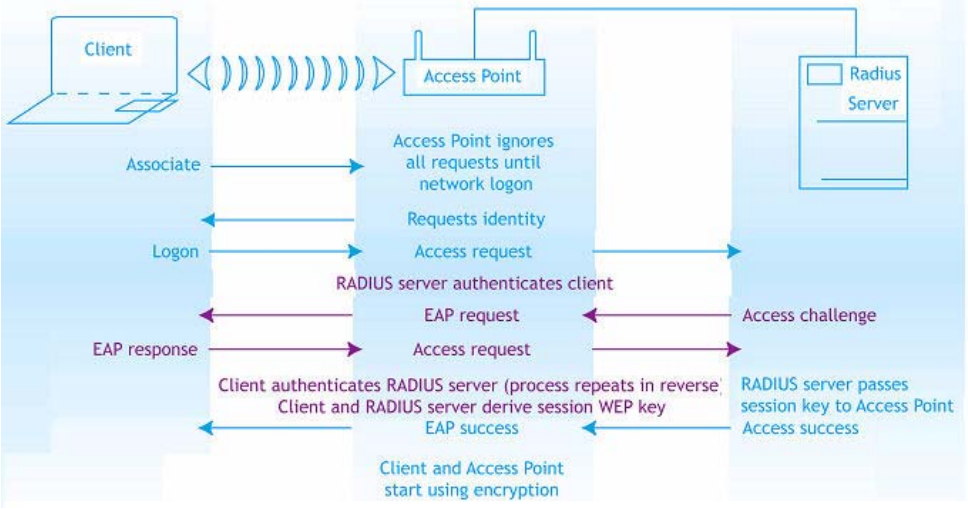
DoS (denial of service) attacks against wireless client station are typically carried out based on the fact that 802.11 management frames and 802.1x authentication protocols have no encryption mechanism and thus can be spoofed. For example, wireless intruders can disrupt the service to a client station by continuously spoofing a 802.11 dis-association or deauthentication frame from the access point to the client station. The 802.11 association state machine as specified by the IEEE standard is illustrated in Figure 17-7 to show how an associated station can be tricked out of the authenticated and associated state by various types of spoofed frames.

Figure 17-7 802.11 Association and Authentication State Machine



Besides the 802.11 authentication and association state attack, there are similar attack scenarios for 802.1x authentication. For example, 802.1x EAP-Failure or EAP-logoff messages are not encrypted and can be spoofed to disrupt the 802.1x authenticated state to disrupt wireless service. See Figure 17-8 for 802.1x authentication and key exchange state change.

Figure 17-8 802.1x User Authentication Process



The Cisco Adaptive Wireless IPS tracks the client authentication process and identifies DoS attack signatures. Incomplete authentication and association transactions trigger the attack detection and statistical signature matching process. Detected DoS attack results in setting off wIPS alarms that include the usual alarm detail description and target device information.

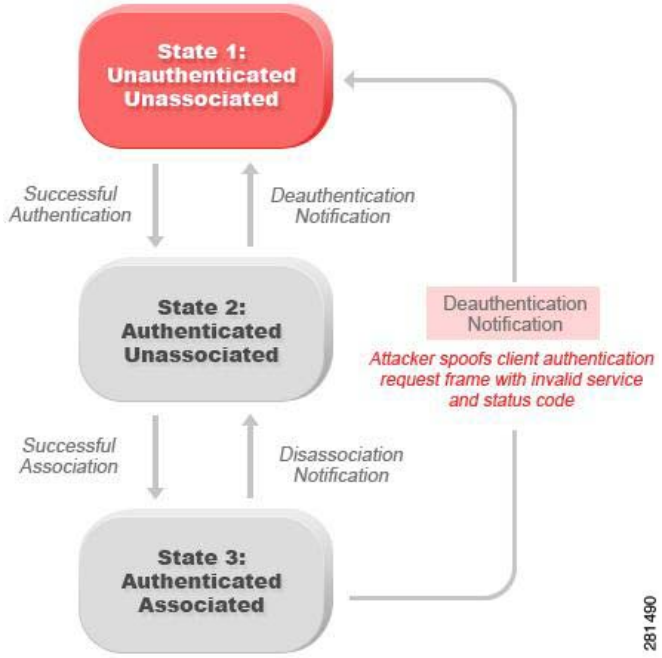
This section describes the DoS attacks against client station and contains the following topics:

Denial of Service Attack: Authentication-Failure Attack

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this client state machine based on the IEEE standard (see Figure 17-9). A successfully associated client remains in State 3 to continue wireless communication. A client in State 1 and in State 2 cannot participate in the WLAN data communication process until it is authenticated and associated to State 3. IEEE 802.11 defines two authentication services: open system authentication and shared key authentication. Wireless clients go through one of these authentication processes to associate with an access point.

Figure 17-9 Client State Machine



A denial of service (DoS) attack spoofs invalid authentication request frames (with bad authentication service and status codes) being sent from an associated client in State 3 to an access point. Upon receipt of the invalid authentication requests, the access point updates the client to State 1, which disconnects client wireless service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of a DoS attack by monitoring for spoofed MAC addresses and authentication failures. This alarm may also indicate an intrusion attempt. When a wireless client fails too many times in authenticating with an access point, the server raises this alarm to indicate a potential intruder attempt to breach security.

Note This alarm focuses on IEEE 802.11 authentication methods, such as open system and shared key. EAP and 802.1x based authentications are monitored by other alarms.

Denial of Service Attack: Block ACK

Alarm Description & Possible Causes

A form of denial of service attack allows an attacker to prevent an 802.11n AP from receiving frames from a specific valid corporate client. With the introduction of the 802.11n standard, a transaction mechanism was introduced which allows a client to transmit a large block of frames at once, rather than dividing them up into segments. To initiate this exchange, the client sends an Add Block Acknowledgement (ADDBA) to the AP, which contains sequence numbers to inform the AP of the size of the block being transmitted. The AP then accepts all frames that fall within the specified sequence (consequently dropping any frames that fall outside of the range) and transmits a BlockACK message back to the client when the transaction has been completed.

To exploit this process, an attacker can transmit an invalid ADDBA frame while spoofing the valid client MAC address. This process causes the AP to ignore any valid traffic transmitted from the client until the invalid frame range has been reached.

wIPS Solution

The wIPS server monitors ADDBA transactions for signs of spoofed client information. When an attacker is detected attempting to initiate a Block ACK attack, an alarm is triggered. We recommend that users locate the offending device and eliminate it from the wireless environment as soon as possible.

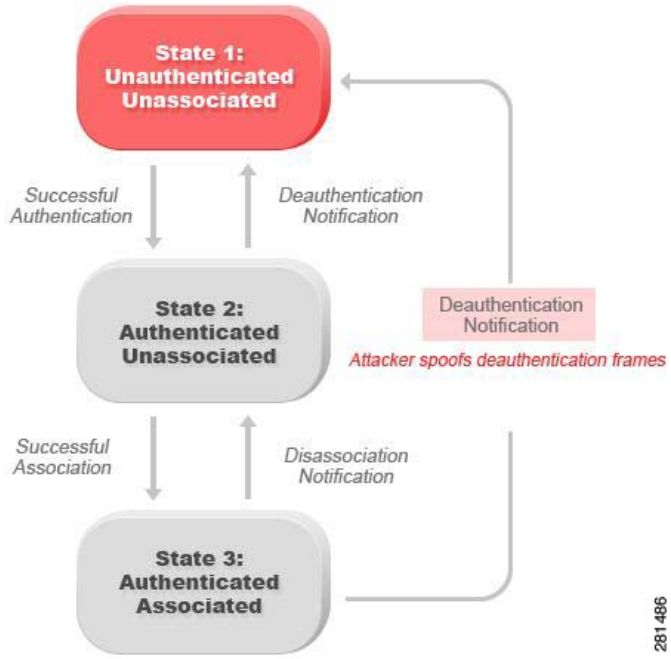
Denial of Service Attack: Deauthentication Broadcast Flood

Attack tool: WLAN Jack, Void11, Hunter Killer

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client remains in State 3 to continue wireless communication. A client in State 1 and State 2 cannot participate in WLAN data communication until it is authenticated and associated to State 3.

Figure 17-10 Client State Machine and Deauthentication Broadcast Attack



A form of DoS attack sends all clients of an access point to the unassociated or unauthenticated State 1 by spoofing deauthentication frames from the access point to the broadcast address. With current client adapter implementation, this form of attack is very effective and immediate in disrupting wireless services against multiple clients. Typically, client stations reassociate and reauthenticate to regain service until the attacker sends another deauthentication frame.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed deauthentication frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security analyst can log onto the access point to verify the current association table status.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide*.

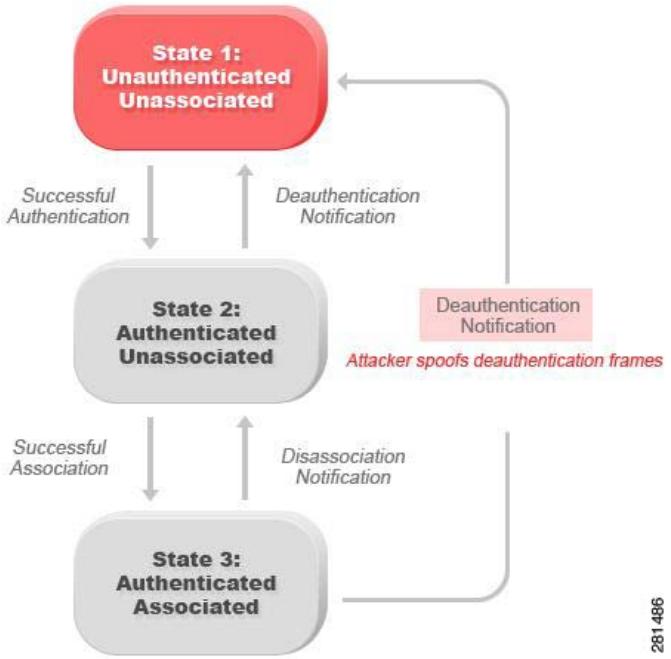
Denial of Service Attack: Deauthentication Flood

Attack tool: WLAN Jack, Void11

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client stays in State 3 to continue wireless communication. A client in State 1 and State 2 cannot participate in WLAN data communication until it is authenticated and associated to State 3.

Figure 17-11 Client State Machine and Deauthentication Flood Attack



A form of DoS attack aims to send an access point client to the unassociated or unauthenticated State 1 by spoofing deauthentication frames from the access point to the client unicast address. With current client adapter implementations, this form of attack is very effective and immediate for disrupting wireless services against the client. Typically, client stations reassociate and reauthenticate to regain service until the attacker sends another deauthentication frame. An attacker repeatedly spoofs the deauthentication frames to keep all clients out of service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed deauthentication frames and tracking client authentication and association states. When the alarm is triggered, the access point and client under attack are identified. The WLAN security officer can log onto the access point to check the current association table status.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide*.

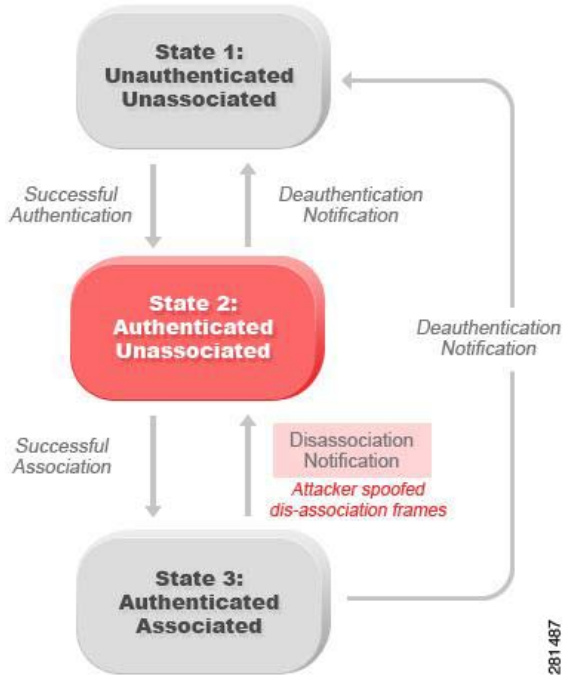
Denial of Service Attack: Disassociation Broadcast Flood

Attack tool: ESSID Jack

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client station stays in State 3 to continue wireless communication. A client station in State 1 and State 2 can not participate in WLAN data communication until it is authenticated and associated to State 3.

Figure 17-12 Client State Machine and Disassociation Broadcast Attack



A form of DoS attack aims to send an access point client to the unassociated or unauthenticated State 2 by spoofing disassociation frames from the access point to the broadcast address (all clients). With current client adapter implementations, this form of attack is effective and immediate for disrupting wireless services against multiple clients. Typically, client stations reassociate to regain service until the attacker sends another disassociation frame. An attacker repeatedly spoofs the disassociation frames to keep all clients out of service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed disassociation frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log onto the access point to check the current association table status.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide*.

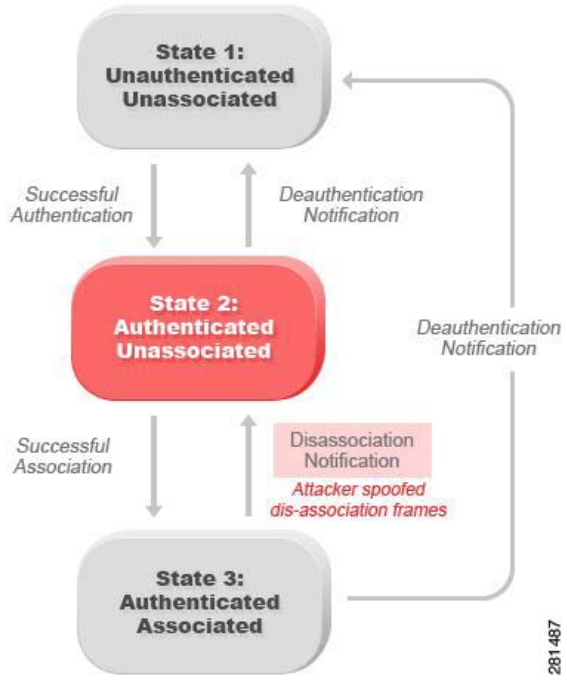
Denial of Service Attack: Disassociation Flood

Attack tool: ESSID Jack

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client stays in State 3 to continue wireless communication. A client in State 1 and State 2 cannot participate in WLAN data communication until it is authenticated and associated to State 3.

Figure 17-13 Client State Machine and Disassociation Flood Attack



A form of DoS attack aims to send an access point to the unassociated or unauthenticated State 2 by spoofing disassociation frames from the access point to a client. With client adapter implementations, this form of attack is effective and immediate for disrupting wireless services against this client. Typically, client stations reassociate to regain service until the attacker sends another disassociation frame. An attacker repeatedly spoofs the disassociation frames to keep the client out of service.

wIPS Solution

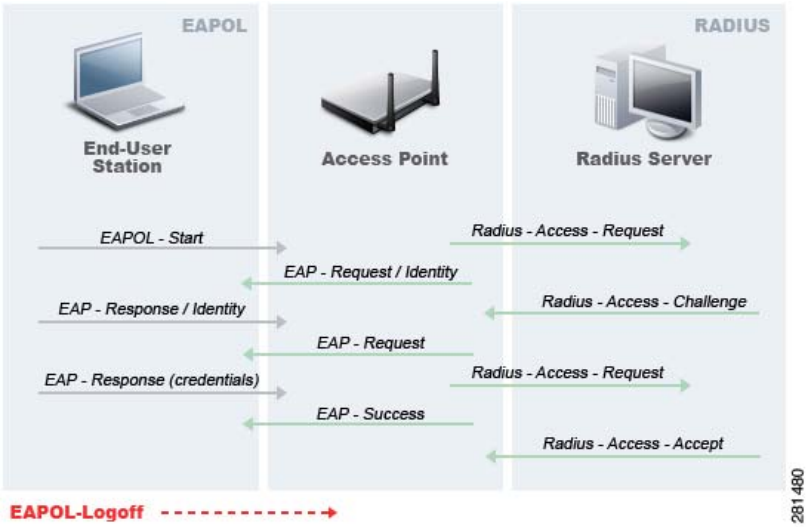
The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed disassociation frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log onto the access point to check the current association table status.

Denial of Service Attack: EAPOL-Logoff Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using Extensible Authentication Protocol (EAP) over LANs or EAPOL. The 802.1x protocol starts with a EAPOL-start frame to begin the authentication transaction. At the end of an authenticated session when a client station logs off, the client station sends an 802.1x EAPOL-logoff frame to terminate the session with the access point.

Figure 17-14 EAPOL-Logoff Protocol and EAPOL-Logoff Attack



Because the EAPOL-logoff frame is not authenticated, an attacker can potentially spoof this frame and log the user off the access point, thus committing a DoS attack. The fact that the client is logged off from the access point is not obvious until it attempts communication through the WLAN. Typically, the disruption is discovered and the client re-associates and authenticates automatically to regain the wireless connection. The attacker can continuously transmit the spoofed EAPOL-logoff frames to be effective on this attack.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking 802.1x authentication states. When the alarm is triggered, the client and access point under attack are identified. The WLAN security officer logs onto the access point to check the current association table status.

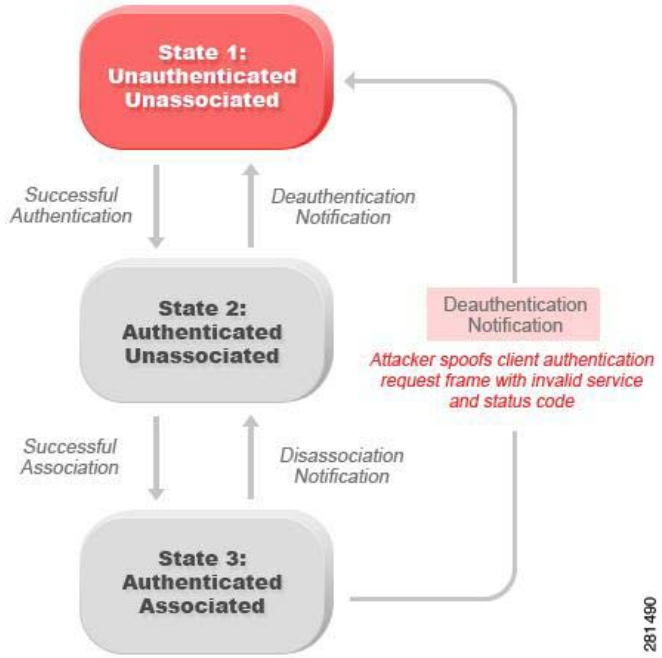
Denial of Service Attack: FATA-Jack Tool

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this state machine based on the IEEE standard. A successfully associated client station stays in State 3 to continue wireless communication. A client station in State 1 and in State 2 cannot participate in the WLAN data communication process until it is

authenticated and associated to State 3. IEEE 802.11 defines two authentication services: open system and shared key. Wireless clients go through one of these authentication processes to associate with an access point.

Figure 17-15 Client State Machine and DoS Attack



A form of DoS attack spoofs invalid authentication request frames (with bad authentication service and status codes) from an associated client in State 3 to an access point. Upon reception of the invalid authentication requests, the access point updates the client to State 1, which disconnects its wireless service.

FATA-jack is one of the commonly used tools to run a similar attack. It is a modified version of WLAN-jack and it sends authentication-failed packets along with the reason code of the previous authentication failure to the wireless station. This occurs after it spoofs the MAC address of the access point. FATA-jack closes most active connections and at times forces the user to reboot the station to continue normal activities.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the use of FATA-jack by monitoring on spoofed MAC addresses and authentication failures. This alarm may also indicate an intrusion attempt. When a wireless client fails too many times in authenticating with an access point, the Cisco Adaptive Wireless IPS raises this alarm to indicate a potential intruder's attempt to breach security.

Note This alarm focuses on 802.11 authentication methods (open system, shared key, and so on). EAP and 802.1x based authentications are monitored by other alarms.

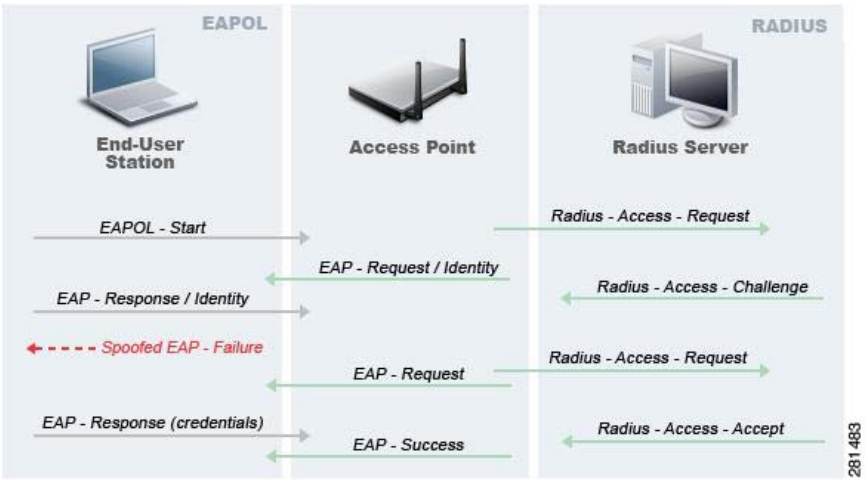
Cisco Management Frame Protection also provides complete proactive protection against frame and device spoofing.

Denial of Service Attack: Premature EAP-Failure

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using Extensible Authentication Protocol over LANs or EAPOL. The 802.1x protocol starts with an EAPOL-Start frame to begin the authentication transaction. When the 802.1x authentication packet exchange is complete with the back-end RADIUS server, the access point sends an EAP-success or EAP-failure frame to the client to indicate authentication success or failure.

Figure 17-16 EAP-Failure Protocol and Premature EAP-Failure Attack



The IEEE 802.1X specification prohibits a client from displaying its interface when the required mutual authentication is not complete. This enables a well-implemented 802.1x client station to avoid being fooled by a fake access point sending premature EAP-success packets.

An attacker keeps the client interface from appearing by continuously spoofing pre-mature EAP-failure frames from the access point to the client to disrupt the authentication state on the client.

wIPS Solution

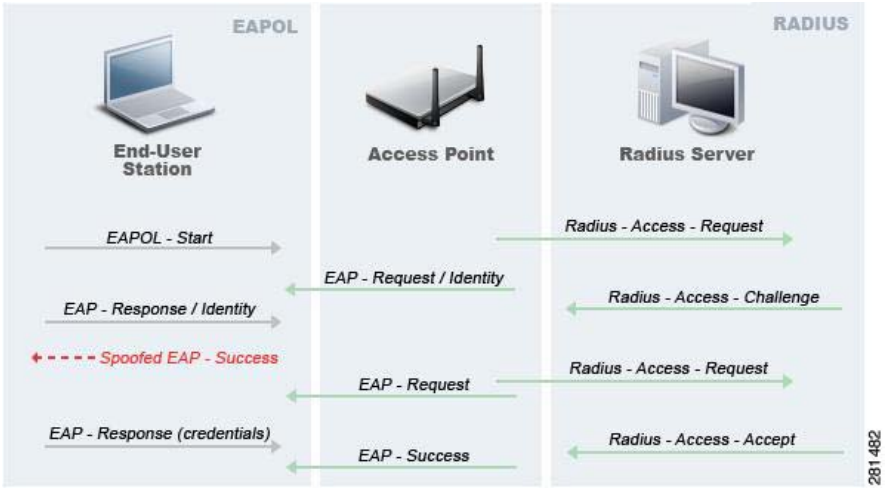
The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking the spoofed premature EAP-failure frames and the 802.1x authentication states for each client station and access point. Find the device and remove it from the wireless environment.

Denial of Service Attack: Premature EAP-Success

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using Extensible Authentication Protocol over LANs or EAPOL. The 802.1x protocol starts with an EAPOL-start frame to begin the authentication transaction. When the 802.1x authentication packet exchange is completed with the back-end RADIUS server, the access point sends an EAP-success frame to the client to indicate a successful authentication.

Figure 17-17 EAP-Success Protocol and EAP-Success Attack



The IEEE 802.1X specification prohibits a client from displaying its interface when the required mutual authentication has not been completed. This enables a well-implemented 802.1x client station to avoid being fooled by a fake access point sending premature EAP-success packets to bypass the mutual authentication process.

An attacker keeps the client interface from appearing by continuously spoofing premature EAP-success frames from the access point to the client to disrupt the authentication state.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking spoofed premature EAP-success frames and the 802.1x authentication states for each client station and access point. Find the device and remove it from the wireless environment.

Intrusion Detection—Security Penetration

A form of wireless intrusion is to breach the WLAN authentication mechanism to gain access to the wired network or the wireless devices. Dictionary attacks on the authentication method is a common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked access point attack on a unsuspicious wireless client may fool the client into associating with faked access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.

These security threats can be prevented if mutual authentication and strong encryption techniques are used. The Cisco Adaptive Wireless IPS looks for weak security deployment practices as well as any penetration attack attempts. The Cisco Adaptive Wireless IPS ensures a strong wireless security umbrella by validating the best security policy implementation as well as detecting intrusion attempts. If such vulnerabilities or attack attempts are detected, the Cisco Adaptive Wireless IPS generates alarms to bring these intrusion attempts to the administrator notice.

This section describes the security penetration attacks and contains the following topics:

- Airsnarf Attack, page 17-25

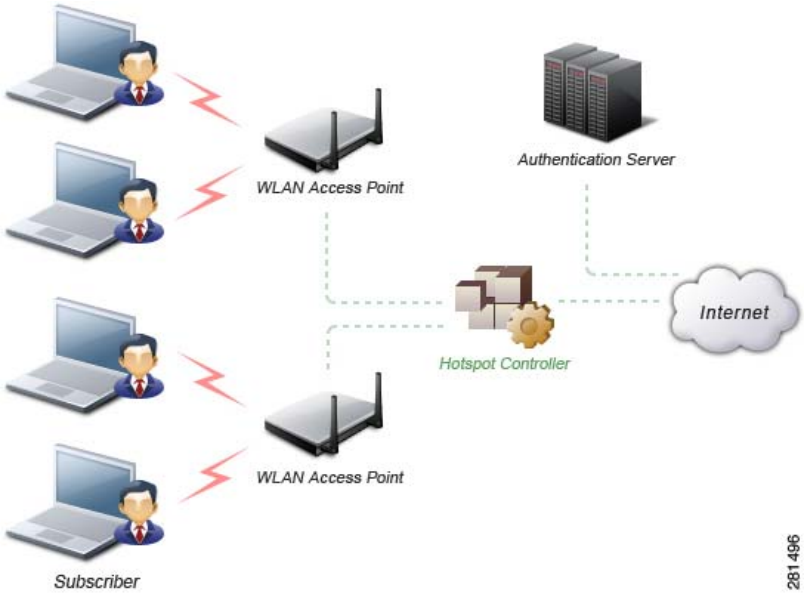
Airsnarf Attack

Alarm Description and Possible Causes

A hotspot is any location where Wi-Fi network access is made available for the general public. Hotspots are found in airports, hotels, coffee shops, and other places where business people tend to congregate. They are important network access services for business travelers.

Customers are able to connect to the legitimate access point and receive service using a wireless-enabled laptop or handheld. Most hotspots do not require the user to have any advanced authentication mechanism to connect to the access point other than popping up a web page for the user to log in. The criterion for entry is dependent only on whether or not the subscriber has paid the subscription fees. In a wireless hotspot environment, no one should be trusted. Due to current security concerns, some WLAN hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user.

Figure 17-18 Basic Components of a WLAN Hotspot Network



The 4 components of a basic hotspot network include:

- Hotspot Subscribers—Valid users with a wireless-enabled laptop or handheld and valid login for accessing the hotspot network.
- WLAN Access Points—Can be SOHO gateways or enterprise level access points depending upon the hotspot implementation.
- Hotspot Controllers—Deals with user authentication, gathering billing information, tracking usage time, filtering functions, and so on. This can be an independent machine or incorporated in the access point itself.
- Authentication Server—Contains the login credentials for the subscribers. Most hotspot controllers verify subscribers credentials with the authentication server.

Airsnarf is a wireless access point setup utility that shows how a hacker can steal username and password credentials from public wireless hotspots.

Airsnarf, a shell script-based tool, creates a hotspot complete with a captive portal where the users enter their login information. Important values such as local network information, gateway IP address, and SSID can be configured within the airsnarf configuration file. This tool initially broadcasts a very strong signal that disassociates the hotspot wireless clients from the authorized access point connected to the Internet. The wireless clients assume that they are temporarily disconnected from the Internet due to some unknown issue and they try to log in again. Wireless clients that associate to the Airsnarf access point receive the IP address, DNS address, and gateway IP address from the rogue Airsnarf access point instead of the legitimate access point installed by the hotspot operator. A web page requests a username and password and the DNS queries are resolved by the rogue Airsnarf access point. The username and password entered are collected by the hacker.

The username and password can be used in any other hotspot location of the same provider anywhere in the nation without the user realizing the misuse. The only case where it could have lesser impact is if the hotspot user is connected using a pay-per-minute usage scheme.

The Airsnarf tool can also penetrate the laptop clients that are unknowingly connected to the Airsnarf access point. The AirSnarf tool can be downloaded by hackers from:

http://airsnarf.shmoo.com/

wIPS Solution

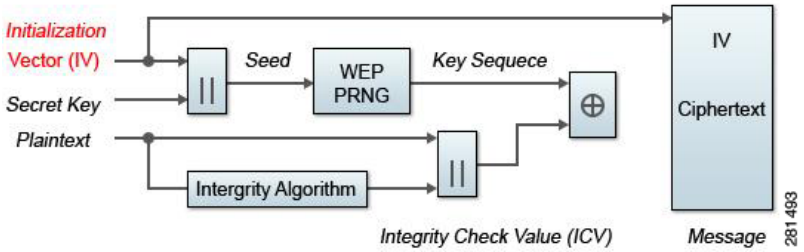
The Cisco Adaptive Wireless IPS detects the wireless device running the AirSnarf tool. Appropriate action must be taken by the administrator to remove the AirSnarf tool from the WLAN environment.

Chopchop Attack

Alarm Description and Possible Causes

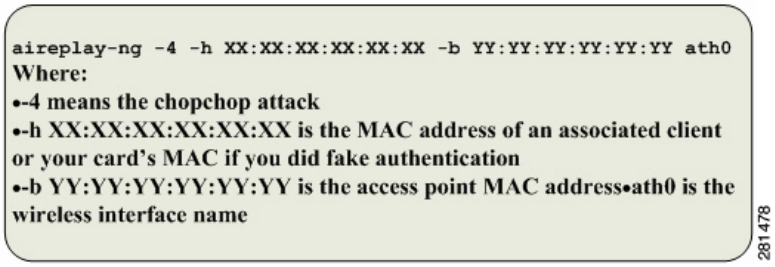
It is well publicized that a WLAN device using a static WEP key for encryption is vulnerable to various WEP cracking attacks. Refer to *Weaknesses in the Key Scheduling Algorithm of RC4 - I* by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information.

Figure 17-19 WEP Encipher Process Block Diagram



A cracked WEP secret key offers no encryption protection for data to be transmitted, leading to compromised data privacy. The WEP key, which is in most cases 64-bit or 128-bit (some vendors also offer 152-bit encryption), is a secret key specified by the user, linked with the 24-bit IV (Initialization Vector). The chopchop tool was written for the Linux operating system by Korek to exploit a weakness in WEP and decrypt the WEP data packet. However, the chopchop tool only reveals the plaintext. The attacker uses the packet capture file of a previously injected packet during the initial phase and decrypts the packet by retransmitting modified packets to the attacked network. When the attack is completed, the chopchop tool produces an unencrypted packet capture file and another file with PRGA (Pseudo Random Generation Algorithm) information determined during the decryption process. The PGRA is then XORed with the cyphertext to obtain the plaintext.

Figure 17-20 Commands for Initiating a Chopchop Attack



Access points that drop data packets shorter than 60 bytes may not be vulnerable to this kind of attack. If an access point drops packets shorter than 42 bytes, aireplay tries to guess the rest of the missing data, as far as the headers are predictable. If an IP packet is captured, it additionally checks if the checksum of the header is correct after guessing the missing parts of it. This attack requires at least one WEP data packet. A chopchop attack also works against dynamic WEP configurations. The Cisco Adaptive Wireless IPS is able to detect potential attacks using the chopchop tool.

wIPS Solution

The Cisco Adaptive Wireless IPS activates an alert when a potential chopchop attack is in progress. WEP should not be used in the corporate environment and appropriate measures should be taken to avoid any security holes in the network and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard.

Day-0 Attack by WLAN Performance Anomaly

Alarm Description and Possible Causes

WLAN performance efficiency is constantly challenged by the dynamics of the RF environment and the mobility of client devices. A closely monitored and well tuned WLAN system can achieve a higher throughput than a poorly managed one. Radio Resource Management (RRM) built into the Cisco Unified Wireless Network monitors and dynamically corrects performance issues found in the RF environment. Further performance anomaly monitoring may be done via the Wireless IPS system. For more information on RRM, see the Cisco NCS online help.

The Cisco Adaptive Wireless IPS ensures WLAN performance and efficiency by monitoring the WLAN on a continued basis and alerting the wireless administrator on early warning signs for trouble. Performance alarms are generated and classified in the following categories in the event of any performance degradation:

- RF Management—The Cisco Adaptive Wireless IPS monitors the physical RF environment that is dynamic and very often the source of WLAN performance problems. While monitoring on the RF environment, the server characterizes the following WLAN fundamentals and reports problems accordingly:
  - Channel interference and channel allocation problems
  - Channel noise and non-802.11 signals
  - WLAN RF service under-coverage area
  - Classic RF hidden-node syndrome

- Problematic traffic pattern—Many WLAN performance problems including the RF multipath problem manifest themselves in the MAC layer protocol transactions and statistics. By tracking and analyzing the wireless traffic, the Cisco Adaptive Wireless IPS is able to spot performance inefficiencies and degradations early on. In many cases, the Cisco Adaptive Wireless IPS can determine the cause of the detected performance problem and suggest counter measures. The Cisco Adaptive Wireless IPS tracks MAC layer protocol characteristics including the following:
  - Frame CRC error
  - Frame re-transmission
  - Frame speed (1, 2, 5.5, 11, ... Mbps) usage and distribution
  - Layer 2 frame fragmentation
  - Access point and station association/re-association/dis-association relationship
  - Roaming hand-off
- Channel or device overloaded—The Cisco Adaptive Wireless IPS monitors and tracks the load to ensure smooth operation with both channel bandwidth limitation or the WLAN device resource capacity. In the event of unsatisfactory performance by the WLAN due to under-provisioning or over-growth, the Cisco Adaptive Wireless IPS raises alarms and offers specific details. RF has no boundaries that could lead to your WLAN channel utilization to increase significantly even when your neighbor installs new WLAN devices in an adjoining channel. The Cisco Adaptive Wireless IPS monitors your WLAN to ensure proper bandwidth and resource provisioning.
- Deployment and operation error—The Cisco Adaptive Wireless IPS scans the airwaves for configuration and operation errors. The following specific areas are continuously monitored:
  - Inconsistent configuration among access points servicing the same SSID
  - Configuration against the principles of best practice
  - Connection problems caused by client/access point mismatch configuration
  - WLAN infrastructure device down or reset
  - Flaws in WLAN device implementation
- IEEE 802.11e and VoWLAN issues—The IEEE 802.11e standard adds QoS (quality of service) features and multimedia support to the existing 802.11 a/b/g wireless standard. This is done while maintaining full backward compatibility with these standards. The QoS feature is critical to voice and video applications. Wireless LAN has limited bandwidth and high overheads as compared to the traditional wired Ethernet. The throughput is reduced for a variety of reasons including the RTS/CTS mechanism, packet fragmentation, packet retransmission, acknowledgements, and collisions.

wIPS Solution

The Cisco Adaptive Wireless IPS has detected a single Performance Intrusion policy violation on a large number of devices in the wireless network. Either the number of devices violating the specific policy in the time period specified are observed or there is a sudden percentage increase in the number of devices as specified in the threshold settings for the alarm. Depending on the Performance Intrusion violation, it is suggested that the devices be monitored and located to carry out further analysis.

For example:

- If the *AP overloaded by stations alarm* is generated by a large number of devices, it may indicate that a hacker has generated thousands of stations and forcing them to associate to the corporate access point. If this occurs, legitimate corporate clients cannot connect to the access point.

- *Excessive frame retries* on the wireless devices may indicate such things as noise, interference, packet collisions, multipath, and hidden node syndrome.

Day-0 Attack by WLAN Security Anomaly

Alarm Description and Possible Causes

The addition of WLANs in the corporate environment introduces a whole new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk of outside penetration and attack. Besides rogue access points, there are many other wireless security vulnerabilities which compromise the wireless network such as misconfigured and unconfigured access points. There can also be DoS (denial of service) attacks from various sources against the corporate network.

The NCS provides automated security vulnerability assessment within the wireless infrastructure that proactively reports any security vulnerabilities or mis-configurations. Further assessment may be done over-the-air via the Wireless IPS system. With the comprehensive suite of security monitoring technologies, the Cisco Adaptive Wireless IPS alerts the user on more than 100 different threat conditions in the following categories:

- User authentication and traffic encryption (Static WEP encryption, VPN, Fortress, Cranite, 802.11i and 802.1x)—Common security violations in this category (authentication and encryption) include mis-configurations, out-of-date software or firmware, and suboptimal choice of corporate security policy.
- Rogue, monitored, and ad-hoc mode devices—Rogue devices must be detected and removed immediately to protect the integrity of the wireless and wired enterprise network.
- Configuration vulnerabilities—Implementing a strong deployment policy is fundamental to a secure WLAN. However, enforcing the policy requires constant monitoring to catch violations caused by mis-configuration or equipment vendor implementation errors. With the increased trend on laptops with built-in Wi-Fi capabilities, the complexity of WLAN configuration extends beyond access points to the user laptops. WLAN device configuration management products can make the configuration process easier, but the need for validation persists especially in laptops with built-in but unused and unconfigured Wi-Fi.
- Intrusion detection on security penetration—A form of wireless intrusion includes breaching the WLAN authentication mechanism to gain access to the wired network or the wireless devices. A Dictionary attack on the authentication method is a very common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked AP attack on a unsuspicious wireless client may fool the client into associating with a fake access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.
- Intrusion detection on denial of service attacks—Wireless DoS (denial of service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLAN at layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example, RF jamming attack with high power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

wIPS Solution

The Cisco Adaptive Wireless IPS has detected a single Security IDS/IPS policy violation on a large number of devices in the wireless network. Either the number of devices violating the specific policy in the time period specified are observed or there is a sudden percentage increase in the number of devices as specified in the threshold settings for the alarm. Depending on the Security IDS/IPS violation, it is suggested that the devices are monitored and located to carry out further analysis to check if they are compromising the Enterprise wireless network in any way (attack or vulnerability). If this is an increase in the number of rogue devices, it may indicate an attack against the network. The WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find it.

If there is a sudden increase in the number of client devices with encryption disabled, it may be necessary to revisit the Corporate Security Policy and enforce users to use the highest level of encryption and authentication according to the policy rules.

Day-0 Attack by Device Performance Anomaly

Alarm Description and Possible Causes

WLAN performance efficiency is constantly challenged by the dynamics of the RF environment and the mobility of client devices. A closely monitored and well-tuned WLAN system can achieve a higher throughput than a poorly managed one. Radio Resource Management built into the Cisco Unified Wireless Network monitors and dynamically corrects performance issues found in the RF environment. Further performance anomaly monitoring may be done via the Wireless IPS system. For more information on RRM, see the Cisco NCS online help.

The Cisco Adaptive Wireless IPS ensures WLAN performance and efficiency by monitoring the WLAN on a continued basis and alerting the wireless administrator on early warning signs for trouble. Performance alarms are generated and classified in the following categories in the event of any performance degradation:

- RF Management—The Cisco Adaptive Wireless IPS monitors the physical RF environment that is dynamic and very often the source of WLAN performance problems. While monitoring on the RF environment, the server characterizes the following WLAN fundamentals and reports problems accordingly:
  - Channel interference and channel allocation problems
  - Channel noise and non-802.11 signals
  - WLAN RF service under-coverage area
  - Classic RF hidden-node syndrome
- Problematic traffic pattern—Many WLAN performance problems including the RF multipath problem manifest themselves in the MAC layer protocol transactions and statistics. By tracking and analyzing the wireless traffic, the Cisco Adaptive Wireless IPS is able to spot performance inefficiencies and degradations early on. In many cases, the Cisco Adaptive Wireless IPS can determine the cause of the detected performance problem and suggest counter measures. The Cisco Adaptive Wireless IPS tracks MAC layer protocol characteristics including the following:
  - Frame CRC error
  - Frame re-transmission
  - Frame speed (1, 2, 5.5, 11, ... Mbps) usage and distribution
  - Layer 2 frame fragmentation

  - Access point and station association/re-association/dis-association relationship
  - Roaming hand-off
- Channel or device overloaded—The Cisco Adaptive Wireless IPS monitors and tracks the load to ensure smooth operation with both channel bandwidth limitation or the WLAN device resource capacity. In the event of unsatisfactory performance by the WLAN due to under-provisioning or over-growth, the Cisco Adaptive Wireless IPS raises alarms and offers specific details. RF has no boundaries that could lead to your WLAN channel utilization to increase significantly even when your neighbor installs new WLAN devices in an adjoining channel. The Cisco Adaptive Wireless IPS monitors your WLAN to ensure proper bandwidth and resource provisioning.
- Deployment and operation error—The Cisco Adaptive Wireless IPS scans the airwaves for configuration and operation errors. The following specific areas are continuously monitored:
  - Inconsistent configuration among access points servicing the same SSID
  - Configuration against the principles of best practice
  - Connection problems caused by client/access point mismatch configuration
  - WLAN infrastructure device down or reset
  - Flaws in WLAN device implementation
- IEEE 802.11e and VoWLAN issues—The IEEE 802.11e standard adds QoS (quality of service) features and multimedia support to the existing 802.11 a/b/g wireless standard. This is done while maintaining full backward compatibility with these standards. The QoS feature is critical to voice and video applications. Wireless LAN has limited bandwidth and high overheads as compared to the traditional wired Ethernet. The throughput is reduced for a variety of reasons including the RTS/CTS mechanism, packet fragmentation, packet retransmission, acknowledgements, and collisions.

To maximize the power of the Cisco Adaptive Wireless IPS, performance alarms can be customized to best match your WLAN deployment specification. For example, if your WLAN is designed for all users to use 5.5 and 11 Mbps speed only, customize the threshold for performance alarm 'Low speed tx rate exceeded' to reflect such an expectation.

wIPS Solution

The Cisco Adaptive Wireless IPS detects a device violating a large number of performance intrusion policies. This device has either generated a large number of performance intrusion violations in the time period specified or there is a sudden percentage increase as specified in the threshold settings for the various alarms. It is suggested that the device is monitored and located to carry out further analysis to check if this device is causing any issues in the overall performance of the network.

For example, if there is a device which has caused an increase in the number of "access points overloaded by stations" and "access points overloaded by utilization" alarms, this could indicate that the access point cannot handle the stations. The administrator may need to reconsider re-deployment of the access points.

Day-0 Attack by Device Security Anomaly

Alarm Description and Possible Causes

The addition of WLANs in the corporate environment introduces a new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. Rogue access points can put the entire corporate network at risk

for outside penetration and attack. Besides rogue access points, there are many other wireless security vulnerabilities which compromise the wireless network such as misconfigured and unconfigured access points. There can also be DoS attacks from various sources against the corporate network.

The NCS provides automated security vulnerability assessment within the wireless infrastructure that proactively reports any security vulnerabilities or mis-configurations. Further assessment may be done over-the-air via the Wireless IPS system. With the comprehensive suite of security monitoring technologies, the Cisco Adaptive Wireless IPS alerts the user on more than 100 different threat conditions in the following categories:

- User authentication and traffic encryption (Static WEP encryption, VPN, Fortress, Cranite, 802.11i and 802.1x)—Common security violations in this category (authentication and encryption) include mis-configurations, out-of-date software or firmware, and suboptimal choice of corporate security policy.
- Rogue, monitored, and ad-hoc mode devices—Rogue devices must be detected and removed immediately to protect the integrity of the wireless and wired enterprise network.
- Configuration vulnerabilities—Implementing a strong deployment policy is fundamental to a secure WLAN. However, enforcing the policy requires constant monitoring to catch violations caused by mis-configuration or equipment vendor implementation errors. With the increased trend on laptops with built-in Wi-Fi capabilities, the complexity of WLAN configuration extends beyond access points to the user laptops. WLAN device configuration management products can make the configuration process easier, but the need for validation persists especially in laptops with built-in but unused and unconfigured Wi-Fi.
- Intrusion detection on security penetration—A form of wireless intrusion includes breaching the WLAN authentication mechanism to gain access to the wired network or the wireless devices. A Dictionary attack on the authentication method is a very common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked AP attack on a unsuspicious wireless client may fool the client into associating with a fake access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.
- Intrusion detection on DoS attacks—Wireless DoS (denial of service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLAN at layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example, RF jamming attack with high power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

wIPS Solution

The Cisco Adaptive Wireless IPS detects a device violating a large number of Security IDS/IPS policies. This device has either generated a number of Security IDS/IPS violations in the time period specified or there is a sudden percentage increase as specified in the threshold settings for the various alarms. The device should be monitored and located to carry out further analysis to check if this device is compromising the Enterprise Wireless Network in any way (attack or vulnerability). If this is a rogue device, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find it.

Device Probing for APs

Some commonly used scan tools include: NetStumbler (newer versions), MiniStumbler (newer versions), MACStumbler, WaveStumbler, PrismStumbler, dStumbler, iStumbler, Aerosol, Boingo Scans, WiNc, AP Hopper, NetChaser, Microsoft Windows XP scans.

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects wireless devices probing the WLAN and attempting association (such as association request for an access point with any SSID).

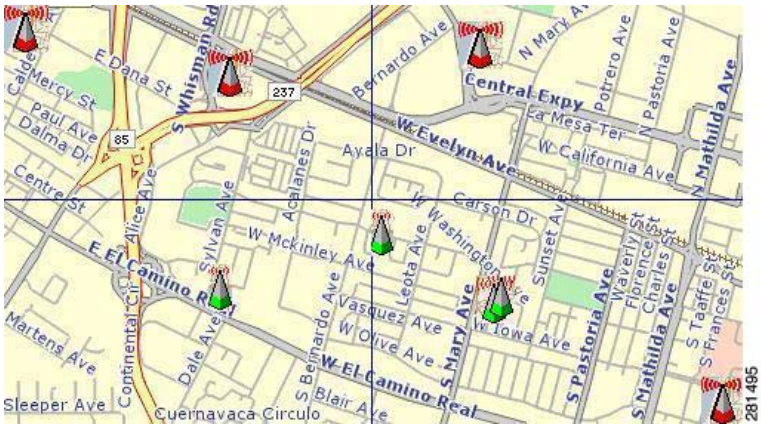
Such devices could pose potential security threats in one of the following ways:

- War-driving, WiLDing (Wireless LAN Discovery), war-chalking, war-walking, war cycling, war-lightrailing, war-busing, and war-flying.
- Legitimate wireless client attempting risky promiscuous association.

War-driving, war-chalking, war-walking, and war-flying activities include:

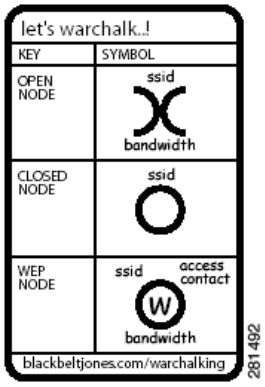
- War-driving—A wireless hacker uses war-driving tools to discover access points and publishes information such as MAC address, SSID, and security implemented on the Internet with the access points geographical location information.

Figure 17-21 802.11 Access Point Locations Posted on the Internet



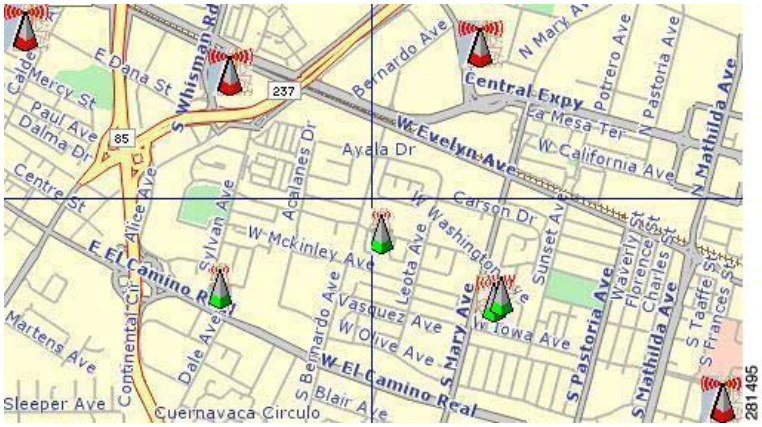
- War-chalking—War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols (Figure 17-22).

Figure 17-22 War-Chalker Universal Symbols



- War-walking—War-walking is similar to war-driving, but the hacker is on foot instead of a car.
- War-flying—War-flying refers to sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet relay chat sessions from an altitude of 1,500 feet on a war-flying trip.

Figure 17-23 802.11 AP Location Posted on the Internet by War-driving Groups



Legitimate Wireless Client Attempting Risky Association

The second potential security threat for this alarm may be more damaging. Some of these alarms could be from legitimate and authorized wireless clients on your WLAN who are attempting to associate with any available access point including your neighbor access point or the more damage-causing rogue access point. This potential security threat can be from a Microsoft Windows XP laptop with a built-in Wi-Fi card or laptops using wireless connectivity tools such as the Boingo client utility and the WiNc client utility. When associated, this client station can be accessed by an intruder leading to a major security breach. Even worse, the client station may bridge the unintended access point with your company wired LAN. Typically, laptops are equipped with built-in Wi-Fi cards and, at the same, are physically attached to your company WLAN for network connectivity. Your wired network is exposed

if the Windows bridging service is enabled on that Windows laptop. To be secure, configure all client stations with specific SSIDs to avoid associating with an unintended access point. Also, consider mutual authentication such as 802.1x and various EAP methods.

The Cisco Adaptive Wireless IPS also detects a wireless client station probing the WLAN for an anonymous association such as an association request for an access point with any SSID) using the NetStumbler tool. The device probing for access point alarm is generated when hackers use the latest versions of the NetStumbler tool. For older versions, the NetStumbler detected alarm is triggered.

NetStumbler is the most widely used tool for war-driving and war-chalking. The NetStumbler website (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or more recent operating systems. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to search shopping malls and retail stores.

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure the access points to not broadcast SSIDs. Use the Cisco Adaptive Wireless IPS to determine which access points are broadcasting (announcing) their SSID in the beacons.

Dictionary Attack on EAP Methods

Alarm Description and Possible Causes

EEE 802.1x provides an EAP framework for wired or wireless LAN authentication. An EAP framework allows flexible authentication protocol implementation. Some implementations of 802.1x or WPA use authentication protocols such as LEAP, MD5, OTP (one-time-password), TLS, and TTLS. Some of these authentication protocols are based on the username and password mechanism in which the username is transmitted without encryption and the password is used to answer authentication challenges.

Most password-based authentication algorithms are susceptible to dictionary attacks. During a dictionary attack, an attacker gains the username from the unencrypted 802.1x identifier protocol exchange. The attacker then tries to guess a user password to gain network access by using every word in a dictionary of common passwords or possible combinations of passwords. A dictionary attack relies on a password being a common word, name, or combination of both with a minor modification such as a trailing digit or two.

A dictionary attack can take place actively online, where an attacker repeatedly tries all the possible password combinations. Online dictionary attacks can be prevented using lock-out mechanisms available on the authentication server (RADIUS servers) to lock out the user after a certain number of invalid login attempts. A dictionary attack can also take place offline, where an attacker captures a successful authentication challenge protocol exchange and then tries to match the challenge response with all possible password combinations. Unlike online attacks, offline attacks are not easily detected. Using a strong password policy and periodically expiring user passwords significantly reduces an offline attack tool's success.

wIPS Solution

The Cisco Adaptive Wireless IPS detects online dictionary attacks by tracking 802.1x authentication protocol exchange and the user identifier usages. When a dictionary attack is detected, the alarm message identifies the username and attacking station MAC address.

The Cisco Adaptive Wireless IPS advises switching username and password based authentication methods to encrypted tunnel based authentication methods such as PEAP and EAP-FAST, which are supported by many vendors including Cisco.

EAP Attack Against 802.1x Authentication

Alarm Description and Possible Causes

IEEE 802.1x provides an Extensible Authentication Protocol (EAP) framework for wired or wireless LAN authentication. An EAP framework allows flexible authentication protocol implementation. Some implementations of 802.1x or WPA use authentication protocols such as LEAP, MD5, OTP (one-time-password), TLS, TTLS, and EAP-FAST. Some of these authentication protocols are based on the username and password mechanism, where the username is transmitted clear without encryption and the password is used to answer authentication challenges.

Most password-based authentication algorithms are susceptible to dictionary attacks. During a dictionary attack, an attacker gains the username from the unencrypted 802.1x identifier protocol exchange. The attacker attempts to guess a user password and gain network access by using every "word" in a dictionary of common passwords or possible combinations of passwords. A dictionary attack relies on the fact that a password is often a common word, name, or combination of words or names with a minor modification such as a trailing digit or two.

Intruders with the legitimate 802.1x user identity and password combination (or valid certificate) can penetrate the 802.1x authentication process without the proper knowledge of the exact EAP-type. The intruder tries different EAP-types such as TLS, TTLS, LEAP, EAP-FAST, or PEAP to successfully log onto the network. This is a trial and error effort because there are only a handful of EAP-types for the intruder to try and manage to get authenticated to the network.

wIPS Solution

The Cisco Adaptive Wireless IPS detects an attempt by an intruder to gain access to the network using different 802.1x authentication types. Take appropriate steps to locate the device and remove it from the wireless environment.

Fake Access Points Detected

Alarm Description and Possible Causes

The Fake AP tool is meant to protect your WLAN acting as a decoy to confuse war-drivers using NetStumbler, Wellenreiter, MiniStumbler, Kismet, and so on. The tool generates beacon frames imitating thousands of counterfeit 802.11b access points. War-drivers encountering a large number of access points cannot identify the real access points deployed by the user. This tool, although very effective in fending off war-drivers, poses other disadvantages such as bandwidth consumption, misleading legitimate client stations, and interference with the WLAN management tools. Running the Fake AP tool in your WLAN is not recommended.

wIPS Solution

The administrator should locate the device running the Fake AP tool and remove it from the wireless environment.

Fake DHCP Server Detected

Alarm Description and Possible Causes

Dynamic Host Configuration Protocol (DHCP) is used for assigning dynamic IP addresses to devices on a network.

DHCP address assignment takes place as follows:

Step 1 The client NIC sends out a DHCP discover packet, indicating that it requires a IP address from a DHCP server.

Step 2 The server sends a DHCP offer packet with the IP address.

Step 3 The client NIC sends a DHCP request, informing the DHCP server that it wants to be assigned the IP address sent by the servers offer.

Step 4 The server returns a DHCP ACK, acknowledging that the NIC has sent a request for a specific IP address.

Step 5 The client interface assigns or binds the initially offered IP address from the DHCP server.

The DHCP server should be a dedicated machine and part of the enterprise wired network or it could be a wireless/wired gateway. Other wireless devices can have the DHCP service running innocently or maliciously so as to disrupt the WLAN IP service. Wireless clients that are requesting an IP address from the DHCP server may then connect to these fake DHCP servers to get their IP address because the clients do not have any means to authenticate the server. These fake DHCP servers may give the clients non-functional network configurations or divert all the client's traffic through them. The hackers can then eavesdrop on every packet sent by the client. With the aid of rogue DNS servers, the hacker could also send the users to fake web page logins to get username and password credentials. It could also give out non-functional and non-routable IP addresses to achieve a DoS attack. This sort of attack is generally against a WLAN without encryption such as hotspots or trade show networks.

wIPS Solution

The Cisco Adaptive Wireless IPS detects such wireless STAs running the DHCP service and providing IP addresses to unaware users.

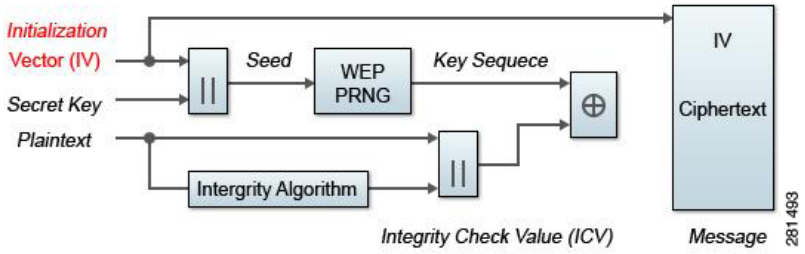
When the client is identified and reported, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the device.

Fast WEP Crack Tool Detected

Alarm Description and Possible Causes

It is well publicized that WLAN devices using static WEP key for encryption are vulnerable to WEP key cracking attack (Refer to *Weaknesses in the Key Scheduling Algorithm of RC4* - I by Scott Fluhrer, Itsik Mantin, and Adi Shamir).

Figure 17-24 WEP Encipherment Block Diagram



The WEP secret key that has been cracked by any intruder results in no encryption protection, thus leading to compromised data privacy. The WEP key that is in most cases 64-bit or 128-bit (few vendors also offer 152-bit encryption) consists of the secret key specified by the user linked with the 24-bit IV (Initialization Vector). The IV that is determined by the transmitting station can be reused frequently or in consecutive frames, thus increasing the possibility of the secret key to be recovered by wireless intruders.

The most important factor in any attack against the WEP key is the key size. For 64-bit WEP keys, around 150 K unique IVs and for 128-bit WEP keys around 500 k to a million unique IVs should be enough. With insufficient traffic, hackers have created a unique way of generating sufficient traffic to perform such an attack. This is called the replay attack based on arp-request packets. Such packets have a fixed length and can be spotted easily. By capturing one legitimate arp-request packet and resending them repeatedly, the other host responds with encrypted replies, providing new and possibly weak IVs.

wIPS Solution

The Cisco Adaptive Wireless IPS alerts on weak WEP implementations and recommends a device firmware upgrade if available from the device vendor to correct the IV usage problem. Ideally, enterprise WLAN networks can protect against WEP vulnerability by using the TKIP (Temporal Key Integrity Protocol) encryption mechanism, which is now supported by most enterprise level wireless equipment. TKIP enabled devices are not subject to any such WEP key attacks.

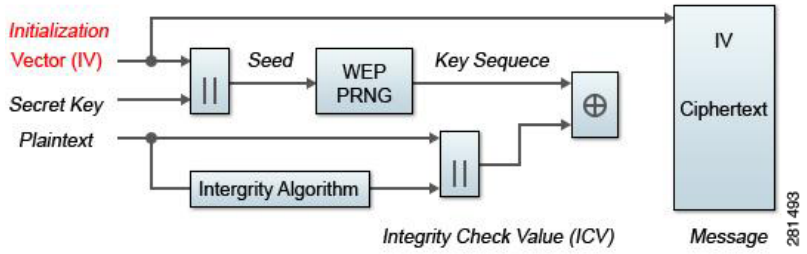
The NCS also provides automated security vulnerability scanning that proactively reports any access points configured to utilize weak encryption or authentication. For more information on automated security vulnerability scanning, see the Cisco NCS online help.

Fragmentation Attack

Alarm Description and Possible Causes

It is well publicized that a WLAN device using a static WEP key for encryption is vulnerable to various WEP cracking attacks. Refer to *Weaknesses in the Key Scheduling Algorithm of RC4 - I* by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information.

Figure 17-25 WEP Encipher Process Block Diagram

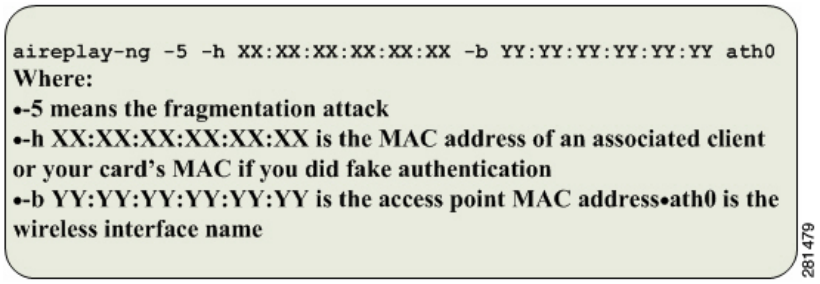


A cracked WEP secret key offers no encryption protection for data to be transmitted which leads to compromised data privacy. The WEP key, which is in most cases 64-bit or 128-bit (few vendors also offer 152-bit encryption), is the secret key specified by the user and linked with the 24-bit IV (Initialization Vector).

According to http://www.aircrack-ng.org/doku.php?id=fragmentation&s=fragmentation, the aircrack program obtains a small amount of keying material from the packet and then attempts to send ARP and/or LLC packets with known information to an access point. If the packet gets successfully echoed back by the access point, then a larger amount of keying information can be obtained from the returned packet. This cycle is repeated several times until 1500 bytes (less in some cases) of PRGA are obtained.

This attack does not recover the WEP key itself, but merely obtains the PRGA. The PRGA can then be used to generate packets with “packetforge-ng” which can be used for various injection attacks.

Figure 17-26 Commands to Run the Fragmentation Attack



The Cisco Adaptive Wireless IPS detects potential fragmentation attacks in progress against the Wi-Fi network.

wIPS Solution

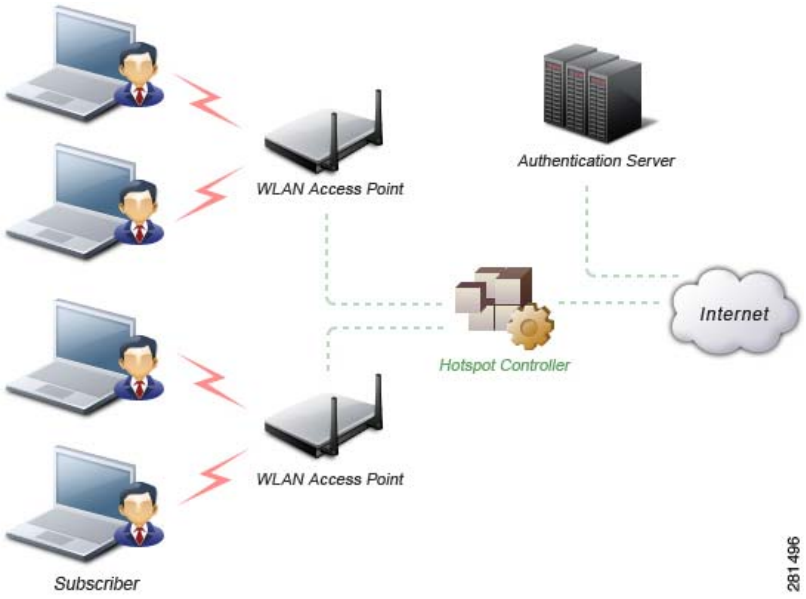
The Cisco Adaptive Wireless IPS alerts on detecting a potential fragmentation attack in progress, and recommends that WEP not be used in the corporate environment and that appropriate measures be taken to avoid any security holes in the network and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard.

Hot-Spotter Tool Detected

Alarm Description and Possible Causes

A hotspot is any location where Wi-Fi network access available for the general public. Hotspots are often found in airports, hotels, coffee shops, and other places where business people tend to congregate. It is currently one of the most important network access service for business travelers. The customer requires a wireless-enabled laptop or handheld to connect to the legitimate access point and to receive service. Most hotspots do not require the user to have an advanced authentication mechanism to connect to the access point, other than using a web page to log in. The criterion for entry is only dependent on whether or not the subscriber has paid subscription fees. In a wireless hotspot environment, no one should trust anyone else. Due to current security concerns, some WLAN hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user.

Figure 17-27 Basic Components of a WLAN Hotspot Network



The four components of a basic hotspot network are:

- Hotspot Subscribers—Valid users with a wireless enabled laptop or handheld and valid login for accessing the hotspot network.
- WLAN Access Points—SOHO gateways or enterprise level access points depending upon the hotspot implementation.
- Hotspot Controllers—Deals with user authentication, gathering billing information, tracking usage time, filtering functions, and so on. This can be an independent machine or can be incorporated in the access point itself.
- Authentication Server—Contains the login credentials for the subscribers. In most cases, hotspot controllers verify subscriber credentials with the authentication server.

"Hotspotter" automates a method of penetration against wireless clients, independent of the encryption mechanism used. Using the Hotspotter tool, the intruder can passively monitor the wireless network for probe request frames to identify the SSIDs of the networks of the Windows XP clients.

After it acquires the preferred network information, the intruder compares the network name (SSID) to a supplied list of commonly used hotspot network names. When a match is found, the Hotspotter client acts as an access point. The clients then authenticate and associate unknowingly to this fake access point.

When the client gets associated, the Hotspotter tool can be configured to run a command such as a script to kick off a DHCP daemon and other scanning against the new victim.

Clients are also susceptible to this kind of attack when they are operating in different environments (home and office) while they are still configured to include the hotspot SSID in the Windows XP wireless connection settings. The clients send out probe requests using that SSID and make themselves vulnerable to the tool.

wIPS Solution

When the rogue access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

Malformed 802.11 Packets Detected

Alarm Description and Possible Causes

Hackers using illegal packets (malformed non-standard 802.11 frames) can force wireless devices to behave in an unusual manner. Illegal packets can cause the firmware of a few vendor wireless NICs to crash.

Examples of such vulnerability includes NULL probe response frame (null SSID in the probe response frame) and oversized information elements in the management frames. These ill-formed frames can be broadcasted to cause multiple wireless clients to crash.

wIPS Solution

The Cisco Adaptive Wireless IPS can detect these illegal packets that may cause some NICs to lock up and crash. Also, wireless clients experiencing blue screen or lock-up problem during the attack period should consider upgrading the WLAN NIC driver or the firmware.

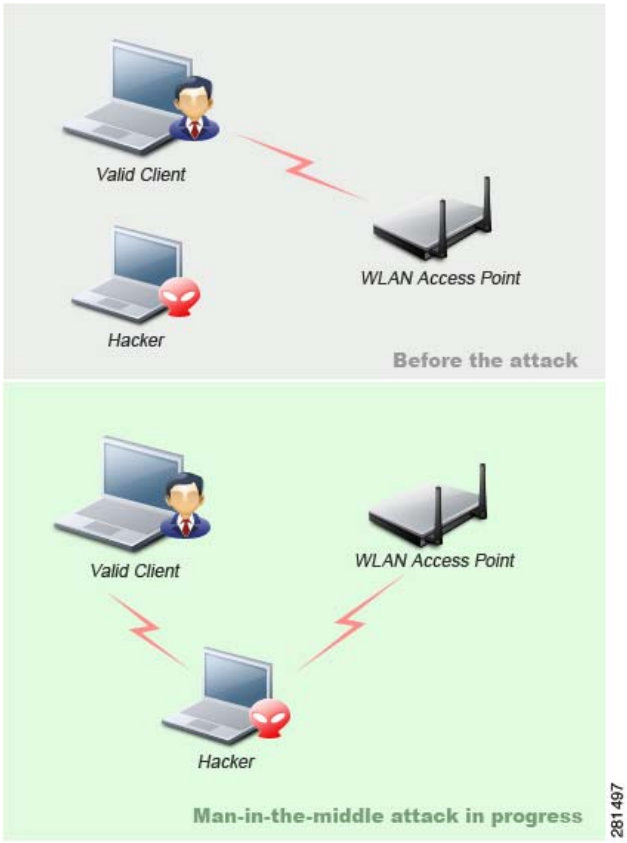
When the client is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use the device locator to locate it.

Man-in-the-Middle Attack

Alarm Description and Possible Causes

A Man-in-the-middle (MITM) attack is one of the most common 802.11 attacks that can lead to confidential corporate and private information being leaked to hackers. In a MITM attack, the hacker can use a 802.11 wireless analyzer and monitor 802.11 frames sent over the WLAN. By capturing the wireless frames during the association phase, the hacker gets IP and MAC address information about the wireless client card and access point, association ID for the client, and the SSID of the wireless network.

Figure 17-28 Man-in-the-Middle Attack



A common MITM attack involves the hacker sending spoofed disassociation or deauthentication frames. The hacker station then spoofs the MAC address of the client to continue an association with the access point. At the same time, the hacker sets up a spoofed access point in another channel to keep the client associated. All traffic between the valid client and access point then passes through the hacker station.

One of the most commonly used MITM attack tools is Monkey-Jack.

wIPS Solution

The Cisco Adaptive Wireless IPS recommends the use of strong encryption and authentication mechanisms to thwart any MITM attacks by hackers. One way to avoid such an attack is to prevent MAC address spoofing by using MAC address exclusion lists and monitoring the RF channel environment.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MITM attacks.

Monitored Device Detected

Alarm Description and Possible Causes

There are some cases in which the access points and STAs activity must be continuously monitored:

- Malicious intruders attempting to hack into the enterprise wired network must be monitored. It is important to keep track of these access points and STAs to help avoid repeated rogue-related and intrusion attempt problems.

- Lost enterprise wireless equipment must be located.
- Vulnerable devices with previous security violations must be monitored.
- Devices used by ex-employees who may have not returned all their wireless equipment must be monitored.

These nodes may be added to the monitor list to alert the wireless administrator the next time the access point or STA shows up in the RF environment.

wIPS Solution

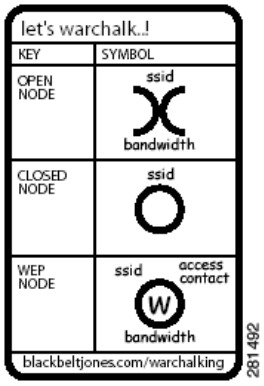
The wireless administrator can add the access point or STA to the monitor list by identifying it as a monitored device on the Cisco Adaptive Wireless IPS.

NetStumbler Detected

Alarm Description and Possible Causes

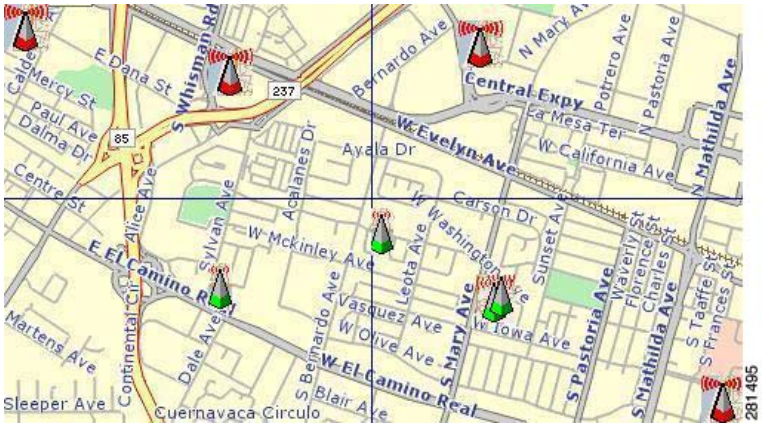
The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (such as an association request for an access point with any SSID) using the NetStumbler tool. The *Device probing for Access Point* alarm is generated when hackers use recent versions of the NetStumbler tool. For older versions, the Cisco Adaptive Wireless IPS generates the *NetStumbler detected* alarm.

Figure 17-29 War-Chalker Universal Symbols



NetStumbler is the most widely used tool for war-driving and war-chalking. A wireless hacker uses war-driving tools to discover access points and to publish their information (MAC address, SSID, security implemented, and so on.) on the Internet with the access points' geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similiar to war-driving, but the hacker is on foot instead of a car. The NetStumbler website (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or later versions. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up email and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.

Figure 17-30 Posted 802.11 Access Point Locations



wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which of your access points is broadcasting an SSID in the beacons.

The NCS also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, see the Cisco NCS online help.

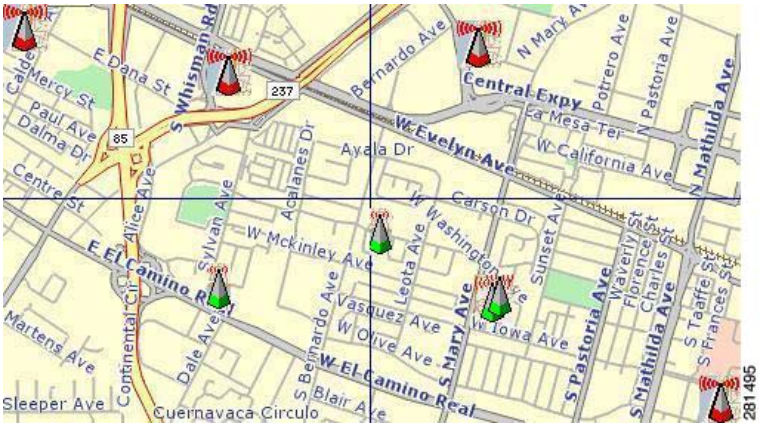
NetStumbler Victim Detected

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (such as association request for an access point with any SSID) using the NetStumbler tool. The Device probing for access point alarm is generated when hackers more recent versions of the NetStumbler tool. For older versions, the Cisco Adaptive Wireless IPS generates the NetStumbler detected alarm.

NetStumbler is the most widely used tool for war-driving, war-walking, and war-chalking. A wireless hacker uses war-driving tools to discover access points and publish their information (MAC address, SSID, security implemented, and so on.) on the Internet with the access point geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similar to war-driving, but the hacker conducts the illegal operation on foot instead of by car. The NetStumbler website (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or later. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers typically use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used, but from a low-flying private plane with high-power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.

Figure 17-31 Posted 802.11 Access Point Locations



The Cisco Adaptive Wireless IPS alerts the user when it observes that a station running Netstumbler is associated to a corporate access point.

wIPS Solution

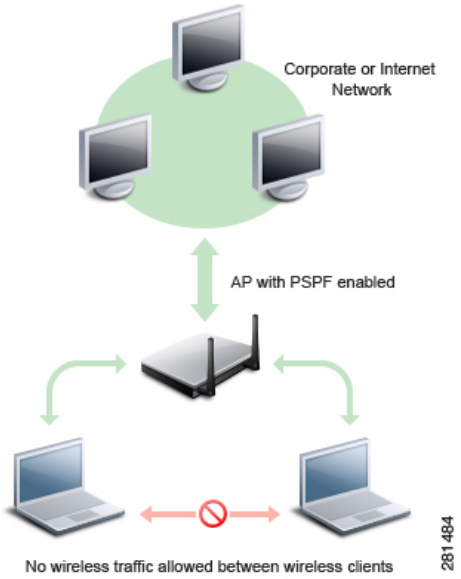
To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which access point is broadcasting its SSID in the beacons.

Publicly Secure Packet Forwarding (PSPF) Violation Detected

Alarm Description and Possible Causes

PSPF is a feature implemented on WLAN access points to block wireless clients from communicating with other wireless clients. With PSPF enabled, client devices cannot communicate with other client devices on the wireless network.

Figure 17-32 PSPF



For most WLAN environments, wireless clients communicate only with devices such as web servers on the wired network. By enabling PSPF it protects wireless clients from being hacked by a wireless intruder. PSPF is effective in protecting wireless clients especially at wireless public networks (hotspots) such as airports, hotels, coffee shops, and college campuses where authentication is null and anyone can associate with the access points. The PSPF feature prevents client devices from inadvertently sharing files with other client devices on the wireless network.

wIPS Solution

The Cisco Adaptive Wireless IPS detects PSPF violations. If a wireless client attempts to communicate with another wireless client, the Cisco Adaptive Wireless IPS raises an alarm for a potential intrusion attack. This alarm does not apply if your WLAN deploys wireless printers or VoWLAN applications because these applications rely on wireless client-to-client communication.

ASLEAP Tool Detected

Alarm Description and Possible Causes

WLAN devices using static WEP key for encryption are vulnerable to the WEP key cracking attack (See *Weaknesses in the Key Scheduling Algorithm of RC4-I* by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information).

Cisco Systems introduced LEAP (Lightweight Extensible Authentication Protocol) to leverage the existing 802.1x framework to avoid such WEP key attacks. The Cisco LEAP solution provides mutual authentication, dynamic per session and per user keys, and configurable WEP session key time out. The LEAP solution was considered a stable security solution and is easy to configure.

There are hacking tools that compromise wireless LAN networks running LEAP by using off-line dictionary attacks to break LEAP passwords After detecting WLAN networks that use LEAP, this tool de-authenticates users which forces them to reconnect and provide their username and password credentials. The hacker captures packets of legitimate users trying to re-access the network. The attacker can then analyze the traffic off-line and guess the password by testing values from a dictionary.

The main features of the ASLEAP tool include:

- Reading live from any wireless interface in RFMON mode with libpcap.
- Monitoring a single channel or performing channel hopping to look for target networks running LEAP.
- Actively deauthenticating users on LEAP networks, forcing them to reauthenticate. This allows quick LEAP password captures.
- Only de-authenticating users who have not already been seen rather than users who are not running LEAP.
- Reading from stored libpcap files.
- Using a dynamic database table and index to allow quick lookups on large files. This reduces the worst-case search time to .0015% as opposed to lookups in a flat file.
- Writing only the LEAP exchange information to a libpcap file.

This could be used to capture LEAP credentials with a device short on disk space (like an iPaq); the LEAP credentials are then stored in the libpcap file on a system with more storage resources to mount the dictionary attack.

The source and Win32 binary distribution for the tool are available at http://asleap.sourceforge.net.

Cisco Systems has developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol which stops these dictionary attacks. EAP-FAST helps prevent man-in-the-middle attacks, dictionary attacks, and packet and authentication forgery attacks. In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is then authenticated using the user-name and password credentials.

Some advantages of EAP-FAST include:

- It is not proprietary.
- It is compliant with the IEEE 802.11i standard.
- It supports TKIP and WPA.
- It does not use certificates and avoids complex PKI infrastructures.
- It supports multiple Operating Systems on PCs and Pocket PCs.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the deauthentication signature of the ASLEAP tool. When detected, the server alerts the wireless administrator. The user of the attacked station should reset the password. The best solution to counter the ASLEAP tool is to replace LEAP with EAP-FAST in the corporate WLAN environment.

The NCS also provides automated security vulnerability scanning that proactively reports any access points configured to utilize weak encryption or authentication. For more information on automated security vulnerability scanning, see the Cisco NCS online help.

Honey Pot AP Detected

Alarm Description and Possible Causes

The addition of WLANs in the corporate environment introduces a whole new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured access points, unconfigured access points, and DoS (denial of service) attacks.

One of the most effective attacks facing enterprise networks implementing wireless is the use of a "honey pot" access point. An intruder uses tools such as NetStumbler, Wellenreiter, and MiniStumbler to discover the SSID of the corporate access point. Then the intruder sets up an access point outside the building premises or, if possible, within the premises and broadcasts the discovered corporate SSID. An unsuspecting client then connects to this "honey pot" access point with a higher signal strength. When associated, the intruder performs attacks against the client station because traffic is diverted through the "honey pot" access point.

wIPS Solution

When a "honey pot" access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

Soft AP or Host AP Detected

Host AP tools: Cqure AP

Alarm Description and Possible Causes

A host-based access point (desktop or a laptop computer serving as a wireless access point) represents two potential threats to enterprise security. First, host based access points are not typically part of the enterprise wireless infrastructure and are likely to be rogue devices which do not conform to the corporate security policy. Second, host-based access points are used by wireless attackers as a convenient platform to implement various known intrusions such as man-in-the-middle, honey-pot access point, access point impersonation, and DoS (denial of service) attacks. Since software tools for turning a desktop or laptop into an access point can be easily downloaded from the Internet, host-based access points are more than just a theoretical threat.

Some laptops are shipped with the Host AP software pre-loaded and activated. When the laptops connect to the enterprise wireless network, they expose the wireless network to the hackers.

wIPS Solution

The Cisco Adaptive Wireless IPS detected soft access point should be treated as a rogue access point as well as a potential intrusion attempt. When the soft access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

Spoofed MAC Address Detected

Spoofing tools may include the following: SMAC, macchanger, and SirMACsAlot.

Alarm Description and Possible Causes

A wireless intruder can disrupt a wireless network using a wide range of available attack tools, many of which are available as free downloads from the Internet. Most of these tools rely on a spoofed MAC address which masquerades as an authorized wireless access point or as an authorized client. By using these tools, an attacker can launch various denial of service (DoS) attacks, bypass access control mechanisms, or falsely advertise services to wireless clients.

wIPS Solution

The Cisco Adaptive Wireless IPS detects a spoofed MAC address by following the IEEE authorized OUI (vendor ID) and 802.11 frame sequence number signature.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide*.

Suspicious After-Hours Traffic Detected

Alarm Description and Possible Causes

One way to detect a wireless security penetration attempt is to match wireless usage against the time when there is not supposed to be any wireless traffic. The wIPS server monitors traffic patterns against the office-hours configured for this alarm to generate alerts when an abnormality is found. Specific suspicious wireless usage sought after by the wIPS server during after-office hours includes the following:

- Client station initiating authentication or association requests to the office WLAN that may indicate security breach attempts.
- Wireless data traffic that may indicate suspicious download or upload over the wireless network.

wIPS Solution

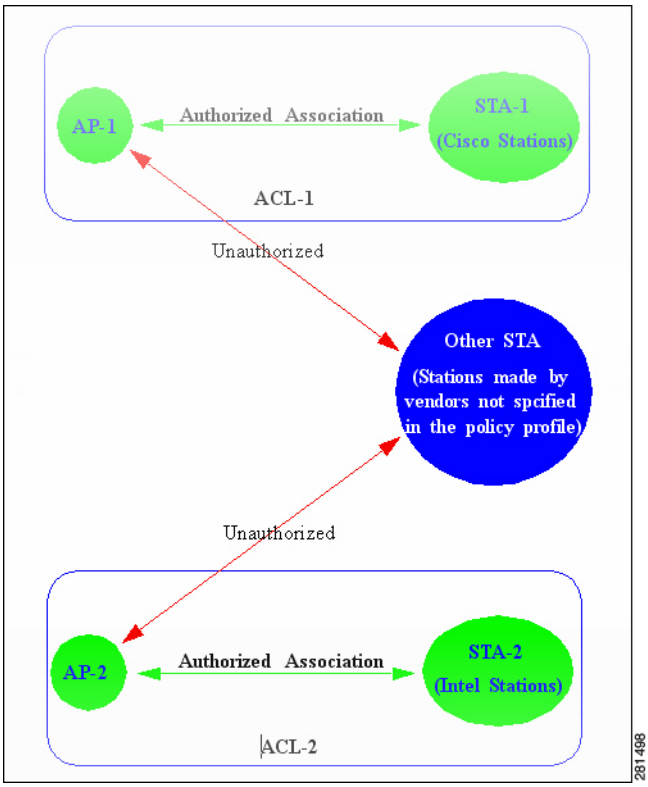
For global wIPS deployment, the configurable office-hour range is defined in local time. The access point or sensor can be configured with a time zone to facilitate management. For the office and manufacturing floor mixed WLAN, one can define one set of office hours for the office WLAN SSID and another set for the manufacturing floor WLAN SSID. If this alarm is triggered, the administrator should look for the devices responsible for the suspicious traffic and remove them from the wireless environment.

Unauthorized Association by Vendor List

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS enables network administrators to include vendor information in a policy profile to allow the system to effectively detect stations on the WLAN that are not made by approved vendors. When such a policy profile is created, the system generates an alarm whenever an access point is associating with a station by an unapproved vendor. See Figure 17-33.

Figure 17-33 Unauthorized Access Point-station Associations Filtered by Station Vendors



As the diagram shows, the access points in ACL-1 should only associate with stations made by Cisco and the access points in ACL-2 can only associate with stations manufactured by Intel. This information is entered in the wIPS system policy profile. Any association between the access points and non-Cisco or non-Intel stations is unauthorized and triggers an alarm.

In the enterprise WLAN environment, rogue stations cause security concerns and undermine network performance. They take up air space and compete for network bandwidth. Since an access point can only accommodate a limited number of stations, it rejects association requests from stations when its capacity is reached. An access point laden with rogue stations denies legitimate stations the access to the network. Common problems caused by rogue stations include connectivity problems and degraded performance.

wIPS Solution

The Cisco Adaptive Wireless IPS automatically alerts network administrators to any unauthorized access point-station association involving non-conforming stations using this alarm. When the alarm has been triggered, the unauthorized station must be identified and actions must be taken to resolve the issue. One way is to block it using the rogue containment.

Unauthorized Association Detected

Alarm Description and Possible Causes

In an enterprise network environment, rogue access points installed by employees do not usually follow the network standard deployment practice and therefore compromise the integrity of the network. They are loopholes in network security and make it easy for intruders to hack into the enterprise wired

network. One of the major concerns that most wireless network administrators face is unauthorized associations between stations in an ACL and a rogue access point. Since data to and from the stations flows through the rogue access point, it leaves the door open for hackers to obtain sensitive information.

Rogue stations cause security concerns and undermine network performance. They take up air space and compete for bandwidths on the network. Since an access point can only serve a certain number of stations, it rejects association requests from stations once its capacity is reached. An access point laden with rogue stations denies legitimate stations access to the network. Common problems caused by rogue stations include disrupted connections and degraded performance.

wIPS Solution

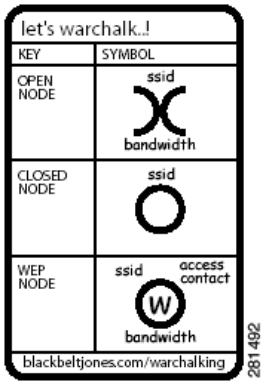
The Cisco Adaptive Wireless IPS can automatically alert network administrators to any unauthorized access point-station association it has detected on the network through this alarm. When the alarm is triggered, the rogue or unauthorized device must be identified and actions must be taken to resolve the reported issue.

Wellenreiter Detected

Alarm Description and Possible Causes

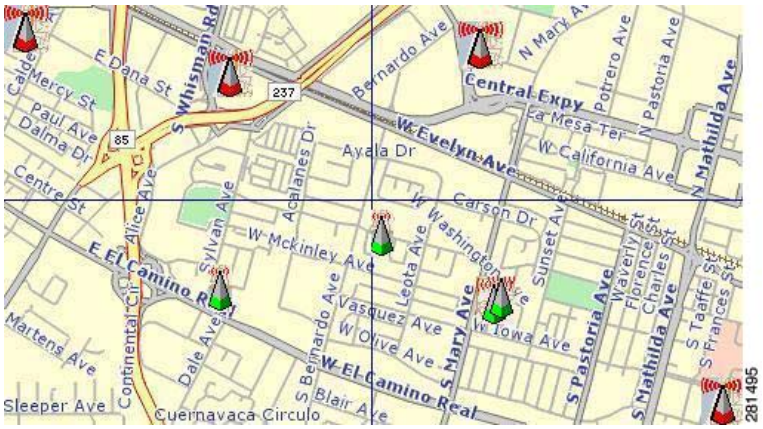
The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (such as association request for an access point with any SSID) using the Wellenreiter tool.

Figure 17-34 War-Chalker Universal Symbols



Wellenreiter is a commonly used tool for war-driving and war-chalking. A wireless hacker uses war-driving tools to discover access points and to publish their information (MAC address, SSID, security implemented, and so on.) on the Internet with the access point geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similar to war-driving, but the hacker is on foot instead of a car. War-walkers like to use Wellenreiter and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used, but from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up email and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.

Figure 17-35 Posted 802.11 Access Point Locations



The tool supports Prism2, Lucent, and Cisco-based cards. The tool can discover infrastructure and ad-hoc networks that are broadcasting SSIDs, their WEP capabilities, and can provide vendor information automatically. It also creates an ethereal/tcpdump-compatible dumpfile and an Application savefile. It also has GPS support. Users can download the tool from http://www.wellenreiter.net/index.html

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which of your access points is broadcasting an SSID in the beacons.

The NCS also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, see the NCS online help.

-

APPENDIX A

Troubleshooting and Best Practices

This appendix identifies and explains any additional troubleshooting or best practices you might find necessary as you implement a particular function.

This appendix includes the following sections:

Troubleshooting Cisco Compatible Extensions Version 5 Client Devices

Two features are designed to troubleshoot communication problems with Cisco Compatible Extension clients: diagnostic channel and client reporting.

Note These features are supported only on Cisco Compatible Extensions Version 5 Client Devices. They are not support for use with non-Cisco Compatible Extensions Version 5 Client Devices or with clients running an earlier version.

Diagnostic Channel

The diagnostic channel feature enables you to troubleshoot problems regarding client communication with a WLAN. When initiated by a client having difficulties, the diagnostic channel is a WLAN configured to provide the most robust communication methods with the fewest obstacles to communication placed in the path of the client. The client and access points can be put through a defined set of tests in an attempt to identify the cause of communication difficulties experienced by the client.

Note Only one WLAN per controller can have the diagnostic channel enabled, and all of the security on this WLAN is disabled.

Configuring the Diagnostic Channel

Follow these steps to configure the diagnostic channel:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address to choose a specific controller.

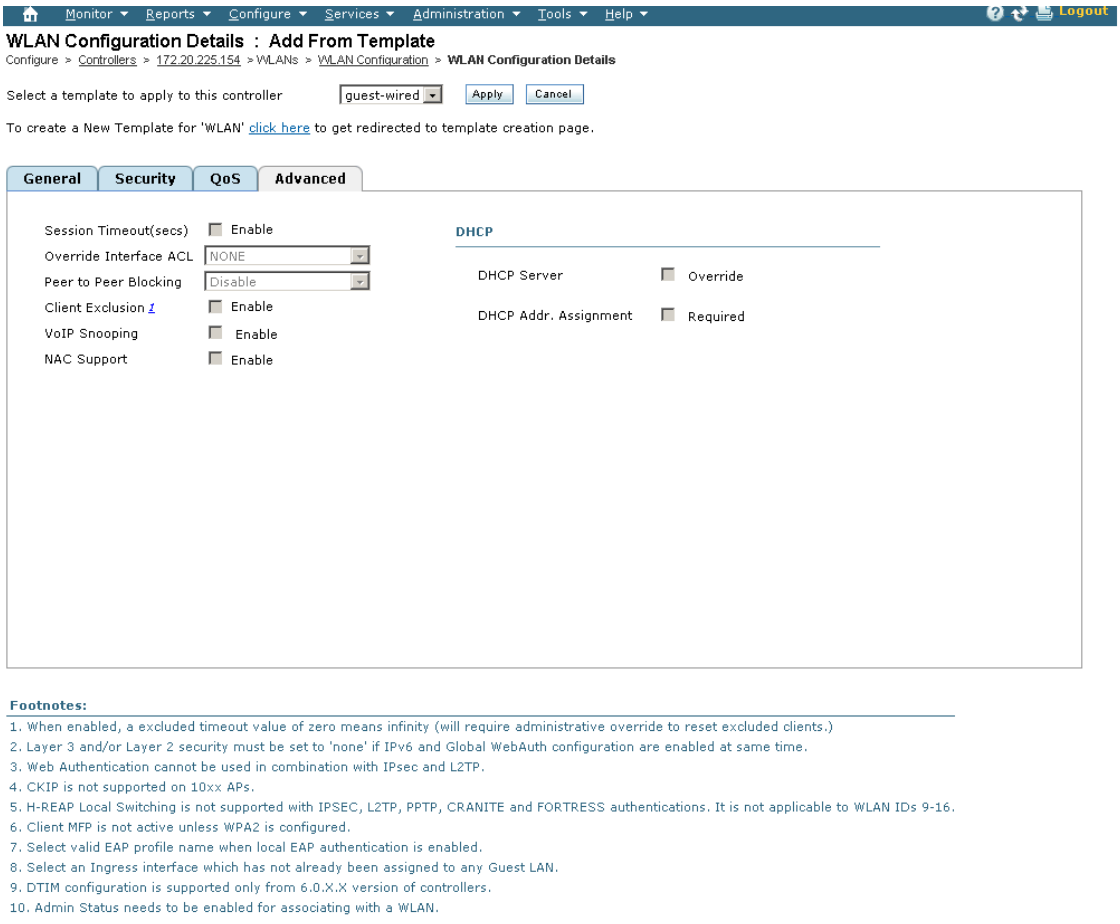
Step 3 Choose **WLANs> WLAN Configuration** from the left sidebar menu.

Step 4 Choose **Add a WLAN** from the Select a command drop-down list to create a new or click the profile name of an existing.

Note We recommend that you create a new WLAN on which to run the diagnostic tests.

Step 5 When the WLANs page appears, click the **Advanced** tab (see Figure A-1).

Figure A-1 WLANs Advanced Tab



Step 6 If you want to enable diagnostic channel troubleshooting on this WLAN, select the **Diagnostic Channel** check box. Otherwise, leave this check box unselected, which is the default value.

Step 7 Click **Save** to commit your changes.

Web Auth Security on WLANs

This section describes the troubleshooting and best practices procedures that are useful when implementing web auth security on WLANs.

Web-auth is a Layer 3 security feature which allows web-based authentication to users on a WLAN. It is used mainly in guest networking scenarios, although not restricted to that usage.

When a WLAN is configured with web-auth security, you are redirected to the login page after passing Layer 2 authentications (static WEP, WPA+PSK, MAC filtering, and so on). The login page is stored on the local device or an external web server, and the page can be modified to allow a customized logo, title, and so on.

After the WLAN is configured with a web-auth WLAN, the HTTP *get* request is sent by the wireless client to the requested website. The controller firewall allows the DNS resolution of the specified URL. After the resolution, the controller interrupts the HTTP packets from the wireless client and redirects to the login page. When the credentials are entered on the login page and submitted, they are authenticated against the local database. If the user is not found in the local database, the configured RADIUS servers are contacted.

Note PAP and CHAP authentication are used between the client and authentication agent. Make sure your RADIUS server supports both of these protocols so web-auth login is allowed.

Upon successful authentication, you are allowed to pass traffic. After three unsuccessful authentication attempts, the client is excluded. This excluded client cannot associate until the exclusion timeout limit is surpassed. The exclusion timeout limit is configured with aggressive load balancing, which actively balances the load between the mobile clients and their associated access points.

Web-auth WLAN is also configured with a pre-authentication access control list (ACL). This ACL is configured the same as a normal ACL but permits access to resources that the client needs prior to authentication. An administrator must use the interface section to apply an ACL to the client after authentication.

A web-auth WLAN can be configured with a session timeout value. This value defines the time the client needs to re-authenticate with the device. If the value is set to zero, which means infinity, the client never re-authenticates unless the logged out option is used. You can access the logout URL at http://<VirtualIP>/logout.html.

Note Disable all pop-up blockers on the client to see the logout page.

Web-auth can be configured in different modes under Layer 3 security. The most commonly used modes of web-auth are as follows:

- Internal Web—Redirection to an internal page using http://<virtual IP /DNS name >/login.html. Customization is available.
- External Web—Redirection to an external URL.

Debug Commands

The following debug commands are allowed:

```
debug client <client-mac-address>
debug pm ssh-tcp enable
debug pm ssh-appgw enable
debug pm rules enable
debug pm config enable

show client detail <client-mac-address>
debug pem event enable
```

Debug Strategy

Use the following strategy for web-auth configured on a WLAN without guest tunneling:

Step 1 Identify a mobile client to work with and write down its wireless MAC address. Use the command **prompt > ipconfig /all** for all MS Windows-based systems.

Step 2 Disable the radio of the mobile client.

Step 3 Enter the following debug commands via a serial console set for high speed (115200) or SSH session to the management port of the controller:

```
debug client <client-mac-address>
debug pm ssh-tcp enable
debug pm ssh-appgw enable
debug pm rules enable
debug pm config enable

show client detail <client-mac-address>

debug pem event enable
debug pem state enable
```

Step 4 Enable the radio and let the client associate. After the client is associated, enter the **show client detail** *client-mac-address* command.

```
$Router1> show client detail 00:0b:85:09:96:10
Client Username ................................ N/A
AP MAC Address.................................. 00:0b:85:09:96:10
Client State.................................... Associated
Wireless LAN Id................................. 1
BSSID........................................... 00:0b:85:09:96:1f
Channel......................................... 11
IP Address...................................... 10.50.234.3
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 0
Client CCX version.............................. 3
Mirroring....................................... Disabled
QoS Level....................................... Silver
Diff Serv Code Point (DSCP)..................... disabled
802.1P Priority Tag............................. disabled
WMM Support..................................... Disabled
Mobility State.................................. Local
Internal Mobility State......................... apfMsMmInitial
Mobility Move Count............................. 0
```

```
--More-- or (q)uit
Security Policy Completed..................... No
Policy Manager State.......................... WEBAUTH_REQD ========**
Policy Manager Rule Created................... Yes
NPU Fast Fast Notified........................ Yes
Last Policy Manager State..................... WEBAUTH_REQD
Client Entry Create Time...................... 67733 seconds
Policy Type................................... N/A
Encryption Cipher............................. None
Management Frame Protection................... No
EAP Type...................................... Unknown
Interface..................................... management
VLAN.......................................... 0
Client Capabilities:
      CF Pollable............................. Not implemented
      CF Poll Request......................... Not implemented
      Short Preamble.......................... Implemented
      PBCC.................................... Not implemented
      Channel Agility......................... Not implemented
      Listen Interval......................... 0
Client Statistics:
      Number of Bytes Received................ 188595
      Number of Bytes Sent.................... 19229
      Number of Packets Received.............. 3074
--More-- or (q)uit
      Number of Packets Sent.................. 76
      Number of Policy Errors................. 0
      Radio Signal Strength Indicator......... -41 dBm
      Signal to Noise Ratio................... 59 dB
Nearby AP Statistics:
        TxExcessiveRetries: 0
        TxRetries: 0
        RtsSuccessCnt: 0
        RtsFailCnt: 0
        TxFiltered: 0
        TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
      ap:09:96:10(slot 1) ....................
antenna0: 48 seconds ago -45 dBm.............. antenna1: 123 seconds ago -128 dBm
```

Step 5 Make sure the pemstate of the client is WEBAUTH_REQD. Open the browser page on the client and look for the following messages:

```
Wed Mar  7 17:59:15 2007: ************* sshpmAddWebRedirectRules: POLICY SEMAPHORE LOCKED
*************
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: mobile station addr is 10.50.234.3
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: RuleID for ms 10.50.234.3 is 44
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: using HTTP-S for web auth (addr:
10.50.234.15).
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: inbound local http rule created for ms
10.50.234.3 local 1.1.1.1.
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: inbound http redirect rule created.
Wed Mar  7 17:59:15 2007: sshpmRuleIndexInsert: adding rule for RuleID 44
Wed Mar  7 17:59:15 2007: sshpmRuleIndexInsert: computed raw hash index 02ad3271 for rule
id 0000002c
Wed Mar  7 17:59:15 2007: sshpmRuleIndexInsert: computed adjusted index 00000c32 for rule
id 0000002c
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: committing rules for ms 10.50.234.3
Wed Mar  7 17:59:15 2007: ************* sshpmPolicyCommitCallback: POLICY SEMAPHORE
UNLOCKED - [unconditionally] ************
Wed Mar  7 17:59:15 2007: sshpmPolicyCommitCallback: called; ContextPtr: 0x2c; Success: 1
Wed Mar  7 17:59:15 2007: ************* sshpmPolicyCommitCallback: POLICY SEMAPHORE
UNLOCKED - [unconditionally] ************
```

```
Wed Mar  7 18:02:32 2007: SshPmAppgw/pm_appgw.c:1234/ssh_pm_appgw_request: New application
gateway request for `alg-http@ssh.com': 10.50.234.3.1153 > 10.50.234.1.80 (nat:
10.50.234.1.80) tcp ft=0x00000000 tt=0x00000000
Wed Mar  7 18:02:32 2007: SshPmAppgw/pm_appgw.c:1239/ssh_pm_appgw_request: Packet
attributes: trigger_rule=0x4ecb, tunnel_id=0x0, trd_index=0xdfffffff,
prev_trd_index=0xdfffffff
Wed Mar  7 18:02:32 2007: SshPmAppgw/pm_appgw.c:1240/ssh_pm_appgw_request: Packet:
Wed Mar  7 18:02:32 2007: 00000000: 4500 0030 0308 4000 8006 0f57 0a32 ea03
E..0..@....W.2..
Wed Mar  7 18:02:32 2007: 00000010: 0a32 ea01 0481 0050 2f42 e3a4 0000 0000
.2.....P/B......
Wed Mar  7 18:02:32 2007: 00000020: 7002 4000 42fe 0000 0204 05b4 0101 0402
p.@.B...........
Wed Mar  7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:403/ssh_pm_st_appgw_start: Calling
redirection callback
Wed Mar  7 18:02:32 2007: SshPmAppgw/pm_appgw.c:155/ssh_appgw_redirect: Application
gateway redirect: 10.50.234.1.80 -> 10.50.234.1.80
Wed Mar  7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:445/ssh_pm_st_appgw_mappings:
Creating application gateway mappings: 10.50.234.3.1153 > 10.50.234.1.80 (10.50.234.1.80)
Wed Mar  7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:102/ssh_pm_appgw_mappings_cb: appgw
connection cached: init flow_index=5967 resp flow_index=5964 event_cnt=718
Wed Mar  7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:493/ssh_pm_st_appgw_mappings_done:
NAT on initiator side
Wed Mar  7 18:02:32 2007:
SshPmStAppgw/pm_st_appgw.c:583/ssh_pm_st_appgw_tcp_responder_stream_done:
ssh_pm_st_appgw_tcp_responder_stream_done: conn->context.responder_stream=0x0
Wed Mar  7 18:02:32 2007:
SshPmStAppgw/pm_st_appgw.c:624/ssh_pm_st_appgw_tcp_responder_stream_done: Opening
initiator stream 10.50.234.1:61611 > 10.76.108.121:2024
Wed Mar  7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:154/ssh_pm_appgw_i_flow_enabled:
Initiator flow mode has now been set.
Wed Mar  7 18:02:32 2007: SshPmAppgw/pm_appgw.c:507/ssh_appgw_tcp_listener_callback: New
initiator stream: src=10.50.234.1:61611, dst=10.76.108.121:2024
Wed Mar  7 18:02:32 2007:
SshPmStAppgw/pm_st_appgw.c:646/ssh_pm_st_appgw_tcp_open_initiator_stream: Initiator stream
opened
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:531/ssh_appgw_http_conn_cb: New TCP
HTTP connection 10.50.234.3.1153 > 10.50.234.1.80
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:535/ssh_appgw_http_conn_cb: Responder
sees initiator as `10.50.234.15.1153'
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:539/ssh_appgw_http_conn_cb: Initiator
sees responder as `10.50.234.1.80'
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:32 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (r) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:32 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:132/ssh_appgw_http_st_wait_input:
appgw_http.c.132: io->src is NULL
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:32 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (r) reading_hdr 1 nmsgs 0
```

```
Wed Mar  7 18:02:32 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:36 2007: SshAppgwHttp/appgw_http.c:132/ssh_appgw_http_st_wait_input:
appgw_http.c.132: io->src is NULL
Wed Mar  7 18:02:36 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
283 bytes (offset 0 data 0)
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 283
bytes:
Wed Mar  7 18:02:41 2007: 00000000: 4745 5420 2f20 4854 5450 2f31 2e31 0d0a  GET /
HTTP/1.1..
Wed Mar  7 18:02:41 2007: 00000010: 4163 6365 7074 3a20 696d 6167 652f 6769  Accept:
image/gi
Wed Mar  7 18:02:41 2007: 00000020: 662c 2069 6d61 6765 2f78 2d78 6269 746d  f,
image/x-xbitm
Wed Mar  7 18:02:41 2007: 00000030: 6170 2c20 696d 6167 652f 6a70 6567 2c20  ap,
image/jpeg,
Wed Mar  7 18:02:41 2007: 00000040: 696d 6167 652f 706a 7065 672c 2061 7070  image/pjpeg,
app
Wed Mar  7 18:02:41 2007: 00000050: 6c69 6361 7469 6f6e 2f78 2d73 686f 636b
lication/x-shock
Wed Mar  7 18:02:41 2007: 00000060: 7761 7665 2d66 6c61 7368 2c20 2a2f 2a0d  wave-flash,
*/*.
Wed Mar  7 18:02:41 2007: 00000070: 0a41 6363 6570 742d 4c61 6e67 7561 6765
.Accept-Language
Wed Mar  7 18:02:41 2007: 00000080: 3a20 656e 2d75 730d 0a41 6363 6570 742d  :
en-us..Accept-
Wed Mar  7 18:02:41 2007: 00000090: 456e 636f 6469 6e67 3a20 677a 6970 2c20  Encoding:
gzip,
Wed Mar  7 18:02:41 2007: 000000a0: 6465 666c 6174 650d 0a55 7365 722d 4167
deflate..User-Ag
Wed Mar  7 18:02:41 2007: 000000b0: 656e 743a 204d 6f7a 696c 6c61 2f34 2e30  ent:
Mozilla/4.0
Wed Mar  7 18:02:41 2007: 000000c0: 2028 636f 6d70 6174 6962 6c65 3b20 4d53   (compatible;
MS
Wed Mar  7 18:02:41 2007: 000000d0: 4945 2036 2e30 3b20 5769 6e64 6f77 7320  IE 6.0;
Windows
Wed Mar  7 18:02:41 2007: 000000e0: 4e54 2035 2e31 3b20 5356 3129 0d0a 486f  NT 5.1;
SV1)..Ho
Wed Mar  7 18:02:41 2007: 000000f0: 7374 3a20 3130 2e35 302e 3233 342e 310d  st:
10.50.234.1.
Wed Mar  7 18:02:41 2007: 00000100: 0a43 6f6e 6e65 6374 696f 6e3a 204b 6565  .Connection:
Kee
Wed Mar  7 18:02:41 2007: 00000110: 702d 416c 6976 650d 0a0d 0a              p-Alive....
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:985/ssh_appgw_parse_request_line: parsing request
line GET / HTTP/1.1
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:1018/ssh_appgw_parse_request_line: internal http
version 3
Wed Mar  7 18:02:41 2007: SshAppgwHttpState/appgw_http_state.c:1155/ssh_appgw_add_method:
caching method 2 for reply 0
Wed Mar  7 18:02:41 2007: SshAppgwHttpState/appgw_http_state.c:1604/ssh_appgw_check_msg:
examining request using service id 34
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:594/ssh_appgw_http_get_dst_host: destination host:
10.50.234.1
```

```
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:1474/ssh_appgw_inject_reply: injecting 404 reply as
msg 0
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:284/ssh_appgw_http_st_write_data:
entering state st_write_data
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 1
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (r) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:1851/ssh_appgw_http_is_inject: next inject is msg# 0
current msg# 0
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:207/ssh_appgw_http_st_inject: entering
state st_inject (r): msgs 0
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:259/ssh_appgw_http_st_inject: closing
connection after inject
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:400/ssh_appgw_http_st_terminate:
entering state st_terminate (r): teardown 0 terminate i: 1 r: 1
Wed Mar  7 18:02:45 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 1
Wed Mar  7 18:02:45 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:45 2007: SshAppgwHttp/appgw_http.c:400/ssh_appgw_http_st_terminate:
entering state st_terminate (i): teardown 0 terminate i: 1 r: 1
Wed Mar  7 18:02:45 2007:
SshAppgwHttp/appgw_http.c:732/ssh_appgw_http_connection_terminate: service HTTP-REDIR: TCP
HTTP connection 10.50.234.3.1153 > 10.50.234.1.80 terminated
Wed Mar  7 18:02:45 2007: SshPmStAppgw/pm_st_appgw.c:1094/ssh_pm_st_appgw_terminate:
terminating appgw instance
```

Step 6 If you do not see the HTTP GET message, the HTTP packet has not reached the controller. After the client completes the redirection, enter your login and submit it.

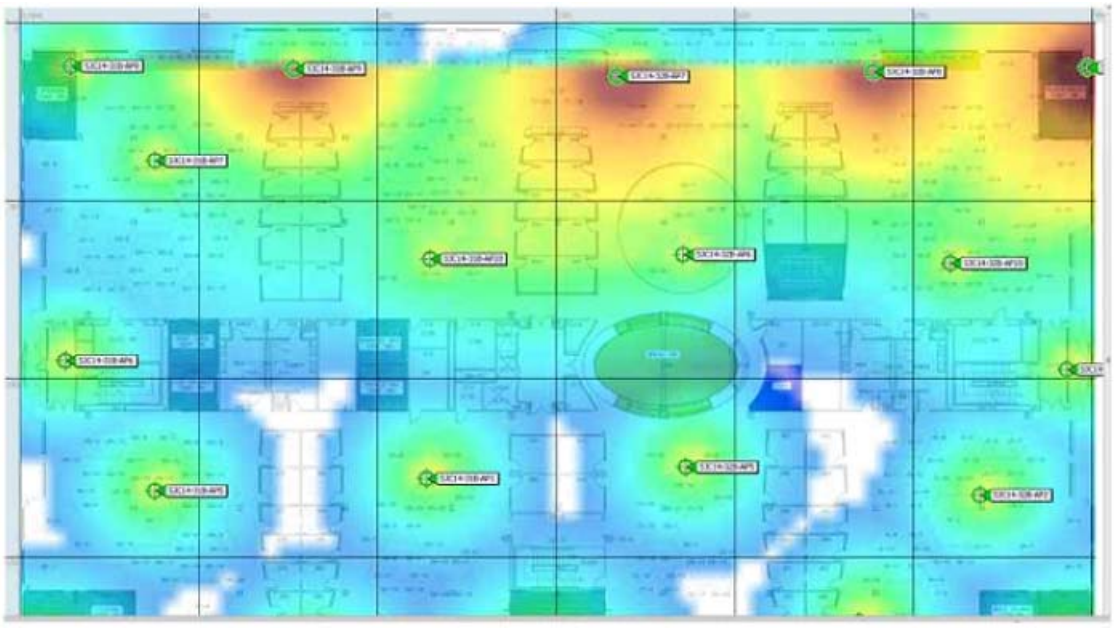
Step 7 Look at the entry of the client in NPUdevshell hapiMmcDebugScbInfoShow (‘client mac address’). If the PEM state is not moved from WEBAUTH_REQD to RUN, a credential problem exists. Check the credentials in the local or RADIUS database (where ever they were configured).

Step 8 When the RUN state appears on the client, perform a check from the client to the gateway and see if traffic is being passed.

RF Heatmap Analysis

Scenario: In some scenarios, you see some wierd heatmaps, where the heatmaps is not consistent all through the AP. One part of the APs shows strong heatmaps and the otherside showing weak heatmaps.

Figure A-2 RF Heatmap Analysis



Analysis: This scenario could be because you could get the neighbor APs RSSI values for one side and not for the other side. Using just one side of the RSSI value predecting the heatmap is not suggested, as there can be a thick wall or wired housing which might lead to incorrect heatmaps.

Scenario: If you are not able to view the dynamic heat map correctly.

Analysis: In case you are not able to view the Dynamic Heatmap correctly, check the following:

- Neighbor AP RSSI values if they are same from both controller and NCS.
- Wait for 20 minutes for the heatmaps to refresh with most latest dynamic heatmap data.
- Check AP Positions.

Best Practices

If the client is not redirected to the login page and you want to avoid DNS resolution in the network, enter **http://***controller-mgmt-ip*. If a redirection occur, the issue is not network related.

Enter **config network web-auth-port** *Port* to define the ports on the controller other than the standard HTTP port (80). The controller does not interrupt secure HTTP or HTTPS (443) even if the port is configured for interrupt.

Troubleshooting RAID Card Configuration

Scenario: When there is an accidental power interruption while the system was operational, the system tries to reboot. During the bootup, the RAID card configuration that was present in the system is lost. Therefore, the system is unable to boot.

Analysis:

Because of the power interruption, the configuration information available in the flash gets corrupted or erased. However, the RAID card backs up the configuration information on the hard drives. But, the RAID card does not pickup the configuration information from the hard drives automatically. You must perform the following steps:

Step 1 Access the CLI version of the RAID Management Tool, WebBIOS, from the serial console.

Step 2 Press CTRL-Y and then type the following command:

-CfgForeign -Import -a0

Step 3 Reboot the server.

APPENDIX B

NCS and End-User Licenses

This appendix provides the end-user license and warranty information that apply to the Cisco NCS. It contains these sections:

NCS Licenses

Before you purchase a Cisco Network Control System (NCS) license, decide on the license type and how many access points need to be supported and licensed.

The four types of licenses for Cisco NCS support different feature levels:

- Cisco NCS Evaluation License
- Cisco NCS Device Count License
- Cisco NCS Upgrade License
- Cisco NCS Migration License

See the "Managing Licenses" section on page 15-131 for information on managing NCS licenses on the GUI.

Types of Licenses

Cisco NCS is deployed through physical or virtual appliances, you use the standard License Center Graphical User Interface to add new licenses, which is locked by the standard Cisco Unique Device Identifier (UDI) or Virtual Unique Device Identifier (VUDI) if you are using a virtual appliance.

The licensing information for existing Cisco WCS deployments are being upgraded to support Cisco NCS 1.0. (While previous Cisco WCS SKUs will be available until September 2011, We recommend that you purchase the new Cisco NCS SKUs outlined in the NCS Ordering Guide (http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps11682/ps11686/guide_c07-653879.html) for a more seamless migration to licensing. This chapter includes information on new Cisco NCS licenses, migrating from Cisco WCS to Cisco NCS, and deploying the free Cisco NCS demonstration license. The types of Cisco Network Control System (NCS) licenses are as follows:

- L-NCS-DEMO-X—Cisco NCS Evaluation License, provides an evaluation license for X number of devices, and for a duration of 30 days. If you need a custom device count or duration, please contact your Cisco representative. For customers who want to download the new full featured, Cisco NCS with Spectrum Integration demonstration license that supports ten access points for up to 30 days. Demo licenses are available at http://www.cisco.com/go/license.

Note The free 30-day trial license is NOT supported by the Cisco Technical Assistance Center (TAC).

- L-NCS-1.0-X—Cisco NCS Enterprise License with Mobility Services Enablement, High availability, and Support for multiple Cisco NCS servers. If you choose the option of ordering the physical appliances, you will be shipped with PRIME-NCS-APL-K9 along with a PAK for the license quantity you ordered (L-NCS-1.0-X). If you choose the virtual appliance option, download the virtual NCS image and get the L-NCS-1.0-X PAK e-mailed to you once it has been ordered.
- L-NCS-1.0-X-ADD —For customer buying new or expansion Cisco NCS licenses running Cisco Unified Wireless Network Software. It is available as L-NCS-1.0-X-ADD option in increments of 50, 100, or 500 lightweight access points. The larger license quantities, specifically 1K, 2.5K, 5K, and 10K are actually shipped in smaller increments to allow the licenses to be split across different NCS instances.

Note When the number of managed devices exceeds the limit of those licensed, NCS generates an alarm. Also, when the user logs into NCS, they are alerted if the licensed access point count has been exceeded.

Note For ADD ON License, you must have one and only one device count license (L-NCS-1.0-X) before stacking “ADD-ON” licenses.

Note Cisco WLSE Express (Model 1030) and CiscoWorks WLSE (Model 1105 or 1133) are NOT supported with this SKU. DO NOT install the CiscoWorks WLSE CDs on the CiscoWorks WLSE Express (Model 1030) appliance or CiscoWorks WLSE (Model 1105 or 1133) because this conversion does not work and is not supported by Cisco Systems.

- NCS-2.0-UPGRADE-X-LIC—For customers upgrading from their existing Cisco NCS licenses to new Cisco NCS licenses. It is available as Cisco NCS UPGRADE in increments of 50, 100, or 500 lightweight access points.
- WCS to NCS Migration—The Cisco NCS uses a single-tier license model. When Cisco WCS BASE or WCS PLUS licenses are being migrated, licenses are mapped to the new Cisco Prime NCS single-tier model. This is a two stage process, Obtaining the XML file from existing WCS deployment and uploading the XML into Cisco Migration Portal. The migration licenses that are generated from the Cisco migration portal. These licenses are mapped to NCS 1.0 licenses of equivalent counts. So an WCS 7.0 Base 500 with Spectrum Expert licenses are converted to an NCS 1.0 500 device license.

Licensing Enforcement

Cisco Unified Wireless Network Releases enforces software based licensing. Customers are prompted to enter license files by all new Cisco NCS SKU families. Existing customers migrating to a later release are also impacted by licensing and should contact their Cisco Sales Representative or TAC to obtain Product Authorization Key (PAK) certificate if they have not already received PAK certificate from Cisco. For more information, refer to the NCS Ordering Guide.

All Cisco NCS licenses can be purchased or acquired directly from Cisco.com via the normal Cisco ordering processes. Cisco Unified Wireless Network Software Releases can be downloaded from Cisco.com or, for a nominal charge, a DVD can be purchased from the NCS-1.0-X or NCS-1.0-X-LIC SKU families. The NCS DVD contains software image of Cisco NCS version 1.0. Customers can select the appropriate Cisco NCS release mode to designate whether they would like to get a Physical Appliance software image(ISO) or a Virtual appliance(OVA) version. The Cisco NCS features and access point quantity are activated after installation by inserting the license file that is tied to the original purchased Cisco NCS SKU. This DVD is shipped via U.S. mail to the purchaser's address.

The Cisco NCS free demonstration license, NCS-DEMO-X is only available as a software download from Cisco.com. Within the 30 day trial period, this free license can be upgraded to one of the non-expiring Cisco NCS SKUs by applying license files generated through the purchase of one of the non-expiring Cisco NCS SKU families.

Product Authorization Key Certificate

All Cisco NCS SKUs require a PAK certificate to register the Cisco NCS license. The PAK is a paper certificate sent via U.S. mail from Cisco Systems upon purchase of the Cisco NCS license. The PAK certificate allows customers to receive a Cisco NCS license. It is used to register the Cisco NCS and generate license files. All customers must go to the PAK registration site listed on their PAK certificate to complete their Cisco NCS registration. The PAK certificate provides clear instructions on how to complete the Cisco NCS licensing process.

Note All customers that purchase Cisco NCS from Cisco.com via download or DVD must activate their Cisco NCS license by registering at the PAK site. Customers receive the PAK via U.S. mail. Cisco NCS is not activated until the PAK registration process is completed.

Determining Which License To Use

You should select the correct license based on your deployment situation, the number of access points to be supported, and Cisco NCS options. Only one type of license can be used on the NCS at one time. For example, if your NCS has a NCS-1.0-X license, you cannot add a NCS-1.0-X-LIC license. You can add to the current license by purchasing a license to increase the access point count. For example, if you have a NCS-1.0-50 license with an access point count of 50 and in a year you need to add more access points, you can buy another NCS-1.0-100 Add-on license with an access point count of 100, apply it to the NCS, and have a NCS with license for 150 access points. You can add a license to increase the number of access points in increments of 50, 100, 500, 1000, 2500, 5000 or 10000.

Installing a License

You need to have the Network Control System license key file to install your license. The key file is distributed to you in an e-mail from Cisco Systems. This file activates the features that you have purchased for your Cisco Network Control System (NCS). Do not edit the contents of the .lic file in any way or you render the file useless.

We strongly recommends that you print the e-mail, save the attachment to a removable media, and store both in a safe place for future use, if needed by either yourself or anyone in your organization.

Before you proceed, make sure that the NCS server software has been installed and configured on the server.

To install the NCS license, follow these steps:

Step 1 Save the license file (.lic) to a temporary directory on your hard drive.

Step 2 Open a supported browser.

Step 3 In the Location or Address text box, enter the following URL, replacing IP address or host name of the NCS server: https://<IP address>.

Step 4 Log in to the NCS server as system administrator. Usernames and passwords are case-sensitive.

Step 5 Choose **Administration > License Center**.

Step 6 Choose **Files > NCS** from the left sidebar menu.

Step 7 Click **Add**. The Add a License File dialog box appears.

Step 8 In the Add a License File dialog box, click **Browse** to navigate to the location where you saved the .lic file.

Step 9 Click **Upload**.

The NCS server imports the license.

During the upload the following items are checked:

- Validity of the license file.
- Matching UDI on the license and NCS system.

If you encounter a problem with the license file, please contact the Cisco Licensing team at 800-553-2447 or licensing@cisco.com.

Backup and Restore License

The license files are saved as part of the backup and restore process, so upgrading NCS will not require reentering of the license files. However, the restore must be on a system with the same UDI for the restored licenses to work. If you have installed an upgraded license on your system, you must reinstall the original license, followed by the upgrade license. To backup the NCS database, see the "Backing Up the NCS Database" section on page 3-7.

Notices and Disclaimers

This chapter/appendix contains notices and disclaimers that pertain to Cisco NCS/Cisco WLAN Controller/whatever other product.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, for example, both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software might not be called “OpenSSL” nor might “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY

THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Disclaimers

All third party trademarks are the property of their respective owners.

End-User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

The following terms of this End User License Agreement ("Agreement") govern Customer's access and use of the Software, except to the extent (a) there is a separate signed agreement between Customer and Cisco governing Customer's use of the Software or (b) the Software includes a separate "click-accept" license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the signed agreement, (2) the click-accept agreement, and (3) this End User License Agreement.

License. Conditioned upon compliance with the terms and conditions of this Agreement, Cisco Systems, Inc. or its subsidiary licensing the Software instead of Cisco Systems, Inc. ("Cisco"), grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) specifically pertaining to the Software and made available by Cisco with the Software in any manner (including on CD-Rom, or on-line).

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such number and types of agent(s), concurrent users, sessions, IP addresses, port(s), seat(s), server(s), site(s), features and feature sets as are set forth in the applicable Purchase Order which has been accepted by Cisco and for which Customer has paid to Cisco the required license fee.

Unless otherwise expressly provided in the Documentation, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Cisco equipment) for communication with Cisco equipment owned or leased by Customer and used for Customer's internal business purposes. NOTE: For evaluation or beta copies for which Cisco does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Cisco retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Cisco, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Accordingly, except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

(i)transfer, assign or sublicense its license rights to any other person or entity, or use the Software on unauthorized or secondhand Cisco equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;

(ii)make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;

(iii)reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction;

(iv)use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Cisco; or

(v)disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Cisco. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by law, and at Customer's written request, Cisco shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Cisco's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Cisco makes such information available.

Software, Upgrades and Additional Copies. For purposes of this Agreement, "Software" shall include (and the terms and conditions of this Agreement shall apply to) computer programs, including firmware, as provided to Customer by Cisco or an authorized Cisco reseller, and any upgrades, updates, bug fixes or modified versions thereto (collectively, "Upgrades") or backup copies of the Software licensed or provided to Customer by Cisco or an authorized Cisco reseller. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Cisco.

Term and Termination. This Agreement and the license granted herein shall remain effective until terminated. Customer may terminate this Agreement and the license at any time by destroying all copies of Software and any Documentation. Customer's rights under this Agreement will terminate immediately without notice from Cisco if Customer fails to comply with any provision of this Agreement. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" and "General Terms Applicable to the Limited Warranty Statement and End User License" shall survive termination of this Agreement.

Customer Records. Customer grants to Cisco and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate license fees, plus the reasonable cost of conducting the audit.

Export. Software and Documentation, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software and Documentation.

U.S. Government End User Purchasers. The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which this End User License Agreement may be incorporated, Customer may provide to Government end user or, if this Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in this End User License Agreement. Use of either the

Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

Limited Warranty

Subject to the limitations and conditions set forth herein, Cisco warrants that commencing from the date of shipment to Customer (but in case of resale by an authorized Cisco reseller, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the warranty period (if any) expressly set forth as applicable specifically to software in the warranty card accompanying the product of which the Software is a part (the "Product") (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to the Documentation. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided AS IS. This limited warranty extends only to the Customer who is the original licensee. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers and licensors under this limited warranty will be (i) replacement of defective media and/or (ii) at Cisco's option, repair, replacement, or refund of the purchase price of the Software, in both cases subject to the condition that any error or defect constituting a breach of this limited warranty is reported to Cisco or the party supplying the Software to Customer, if different than Cisco, within the warranty period. Cisco or the party supplying the Software to Customer may, at its option, require return of the Software as a condition to the remedy. In no event does Cisco warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions. This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Cisco or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; or (d) is licensed, for beta, evaluation, testing or demonstration purposes for which Cisco does not charge a purchase price or license fee.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY CISCO, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

General Terms Applicable to the Limited Warranty Statement and End User License Agreement

Disclaimer of Liabilities. REGARDLESS WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL,

INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Cisco's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim or if the Software is part of another Product, the price paid for such other Product. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Customer agrees that the limitations of liability and disclaimers set forth herein will apply regardless of whether Customer has accepted the Software or any other product or service delivered by Cisco. Customer acknowledges and agrees that Cisco has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

The validity, interpretation, and performance of this Warranty and End User License shall be controlled by and construed under the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of laws, and the State and federal courts of California shall have jurisdiction over any claim arising under this Agreement. The parties specifically disclaim the UN Convention on Contracts for the International Sale of Goods. Notwithstanding the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement shall remain in full force and effect. Except as expressly provided herein, this Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any purchase order or elsewhere, all of which terms are excluded. This Agreement has been written in the English language, and the parties agree that the English version will govern.

Supplemental License Agreement

Cisco Network Control System (NCS)

IMPORTANT-READ CAREFULLY

You have agreed to the Cisco System, Inc. End User License Agreement (“EULA”) that governs your access and use of the Cisco Network Control System ("NCS"). This supplemental license agreement (this "supplement") contains additional terms and conditions.

Capitalized terms used and but not defined in this supplement have the meanings as defined in the EULA. To the extent of a conflict between the provisions of this supplement and the EULA, this supplement takes precedence.

By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this supplement. If Customer does not agree to the terms of this supplement, Customer may not install, download, or otherwise use the Software.

Restrictions on Managed Access Point and Devices

Customer may not use the Software unless:

- Customer obtains a NCS limited license by placing a Purchase Order for a NCS license for a specific number of access points, having the Purchase Order accepted by Cisco, and paying to Cisco the required license fee; or

- Customer obtains a NCS demonstration license by registering and downloading the Software for demonstration purposes in accordance with the Cisco Data Sheet for the Cisco Wireless Control System (the "NCS Data Sheet").

If Customer obtains a NCS limited license, Customer may not use the Software to manage more access points than those identified in the Software's Cisco SKU or the product description on Customer's accepted, paid Purchase Order plus those identified in the Software's Cisco SKUs or the product descriptions on Customer's prior accepted, paid Purchase Orders.

If Customer obtains a NCS demonstration license, Customer may not use the Software to manage more than the number of access points identified for the Cisco NCS demonstration license in the NCS Data Sheet.

Customer may use the Software only to manage those devices identified as managed devices in the product specifications section of NCS Data Sheet.

Server Restrictions

Customer may install and run the Software on multiple servers if the Software's Cisco SKU or product description on Customer's accepted, paid Purchase Order identifies the product as an enterprise or "ent" license. Otherwise, Customer may install and run the Software on only a single server.

Third-Party Proprietary Software

The Software includes proprietary software and technology from Cisco's suppliers. Some suppliers are intended third-party beneficiaries of the EULA and this supplement. Third-party-beneficiary suppliers include: (a) Hifn, Inc.; (b) Wind River Systems, Inc. and its suppliers; and (c) any other supplier Cisco identifies as a third-party beneficiary in the Documentation or additional supplements. These suppliers may enforce, and are express beneficiaries of, the EULA and this supplement. However, they are not in any contractual relationship with Customer.

The limited warranty in the EULA is made only by Cisco and is disclaimed by all Cisco suppliers. Cisco and any Cisco supplier may obtain injunctive relief if Customer's use of the Software is in violation of any license restrictions.

Open-Source Software

The Software includes certain open-source software. Despite anything to the contrary in the EULA or this supplement, the open-source software is governed by the terms and conditions of the applicable open-source license. The open-source software, the applicable open-source licenses and other open-source notices may be identified in the Documentation or in a README file accompanying the Software. Customer agrees to comply with all such licenses and other notices.

Other Terms and Conditions

The terms of the EULA and this supplement may be enforced by license registration and other software tools.

APPENDIX C

Cisco NCS Server Hardening

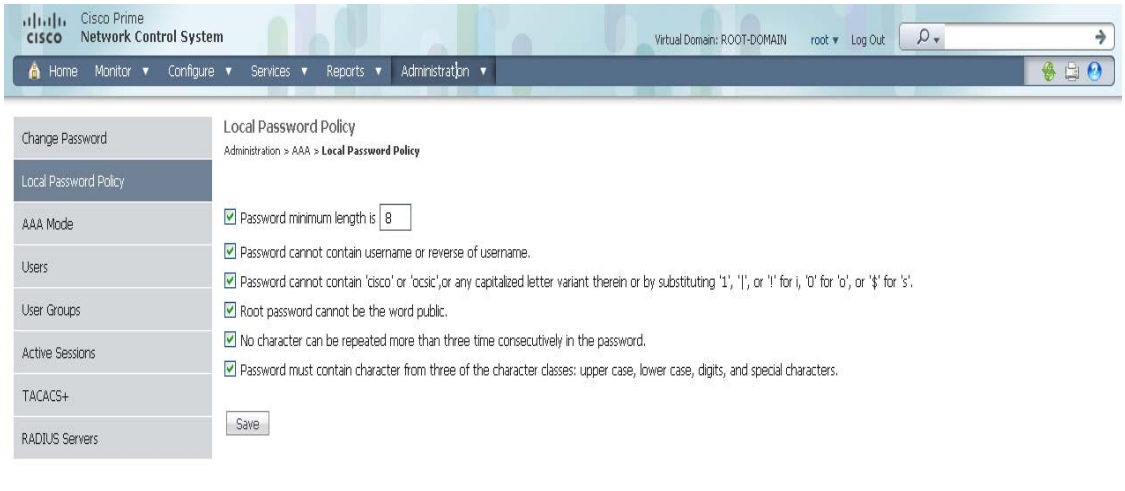
This appendix provides an instructional checklist for hardening a NCS server. Ideally, the goal of a hardened server is to leave it exposed on the Internet without any other form of protection. This describes the hardening of NCS, which requires some services and processes exposed to function properly. Think of it as NCS Best Practices. Hardening of NCS involves disabling unnecessary services, removing and modifying registry key entries, and applying appropriate restrictive permissions to files, services, and end points.

This appendix contains the following sections:

NCS Password Handling

You can configure additional authentication by configuring the **Local Password Policy** parameters. Select the check boxes if you want the configurations to be enabled.

Figure C-1 Local Password Policy



The following configurations are added for additional authentication:

- You can configure the minimum length of the password.

- You can configure if you want to allow the username or reverse of the username to be part of the password.
- You can configure if the password can contain 'cisco', 'ocsic', or any capitalized letter variant therein or by substituting '1', 'l', or '!' for i, '0' for 'o', or '$' for 's'.
- You can configure if the root password can be the word **public**.
- You can configure if a character can be repeated more than three times consecutively in the password or not.
- You can configure if the password must contain character from three of the character classes: upper case, lower case, digits, and special characters.

Setting Up SSL Certification

The Secure Socket Layer (SSL) Certification is to ensure secure transactions between a web server and the browsers. Installing the DoD Certificates allows your Web browser to trust the identity and provide secure communications which are authenticated by Department of Defense (DoD).

These certificates are used to validate the identity of the server or website and are used to generate the encryption key used in the SSL. This encryption protects the information being passed between the server and the client.

SSL Certification involves the following topics:

- Setting Up SSL Client Certification, page C-2
- Setting Up SSL Server Certification, page C-3

Setting Up SSL Client Certification

Follow the below steps to setup the SSL Client Certificate Authentication using DoD certificates:

Note As a prerequisite, to create the SSL Certificates, you would require “KeyTool” available in JDK. KeyTool is a command line tool to manage keystores and the certificates.

Step 1 Create SSL Client Certificate using the below command.

```
% keytool -genkey -keystore nmsclientkeystore -storetype pkcs12 -keyalg RSA -keysize 2048
-alias nmsclient -dname "CN=nmsclient, OU=WNBU, O=Cisco, L=San Jose, ST=CA, C=US"
-storepass nmskeystore
```

Note Provide the Key Algorithm as RSA and KeySize as 1024 or 2048.

Step 2 Generate the Certificate Signing Request (CSR) using the below command.

```
% keytool -certreq -keyalg RSA -keysize 2048  -alias nmsclient -keystore nmsclientkeystore
-storetype pkcs12 -file <csrfilename>
```

Note Provide the Key Algorithm as RSA and KeySize as 1024 or 2048 and provide a certificate file name.

Step 3 Send the generated CSR file to DoD. The DoD issues the corresponding signed certificates.

Note The CSR reply is through dod.p7b file. In addition you should also receive the root CA certificates.

Note Please makes sure to retrieve the PKCS7 encoded certificates; Certificate Authorities provide an option to get the PKCS7 encoded certificates.

Step 4 Import the CSR reply in the Keystore using the command:

```
% keytool -import dod.p7b -keystore nmsclientkeystore -storetype pkcs12
-storepass nmskeystore
```

Step 5 Check the formats of root CA certificates received, they must be base 64 encoded. If they are not base 64 encoded, use the OpenSSL command to convert them to base 64 encoded format.

```
% openssl x509 -in rootCA.cer -inform DER -outform PEM -outfile rootCA.crt
% openssl x509 -in DoD-sub.cer -inform DER -outform PEM -outfile rootCA.crt
```

Note Convert both root CA certificate and sub-ordinate certificates received.

In case you received both root CA certificate and the sub-ordinate certificate, you have to bundle them together using the below command:

```
% cat DoD-sub.crt > ca-bundle.crt
% cat DoD-rootCA.crt >> ca-bundle.crt
```

Step 6 To setup SSL Client Authentication using these certificates, enable SSL Client Authentication in Apache in the **ssl.conf** file located in <NCS_Home>/webnms/apache/ssl/backup/ folder.

```
SSLCACertificationPath conf/ssl.crt
SSLCACertificationFile conf/ssl.crt/ca-bundle.crt
SSLVerifyClient  require
SSLVerifyDepth 2
```

Note SSLVerifyDepth depends on the level of Certificate Chain. In case you have only 1 root CA certificate, this should be set to 1. In case you have a certificate chain (root CA and subordinate CA), this should be set to 2.

Step 7 Install the DoD root CA certificates in NCS.

Step 8 Import the nmsclientkeystore in your browser.

Setting Up SSL Server Certification

To setup the SSL Server Certificate using DoD certificates, follow these steps:

Step 1 Generate the Certificate Signing Request (CSR).

```
% keyadmin -newdn  genkey <csrfilename>
```

Step 2 Send the generated CSR file to DoD. The DoD issues the corresponding signed certificates.

Note The CSR reply is through dod.p7b file. In addition you should also receive the root CA certificates.

Note Please makes sure to retrieve the PKCS7 encoded certificates; Certificate Authorities provide an option to get the PKCS7 encoded certificates.

Step 3 Import the Signed Certificate using the below command in the Keytool:

```
% keyadmin -importsignedcert <dod.p7>
```

Note The NCS stores the self-signed certificate at /opt/CSCOncs/httpd/conf/ssl.crt. The imported certificates/keys are stored at /opt/CSCOncs/migrate/restore.

INDEX

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z