Cisco Adaptive Wireless Intrusion Prevention System Configuration Guide Release 6.0

June 2009

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-19650-01

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.

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.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Adaptive Wireless Prevention System Configuration Guide

CONTENTS

CHAPTER 6

CHAPTER 7

CHAPTER 8

CHAPTER 1

Overview

This chapter describes the role of the Cisco 3300 Series Mobility Services Engine and one of its services, the Cisco Adaptive Wireless Intrusion Prevention System (wIPS) within the overall Cisco Unified Wireless Network (CUWN).

This chapter contains the following sections:

- Overview of wIPS, page 1-2
- Differences Between Controller IDS and Adaptive wIPS, page 1-6
- Configuration Guide Overview, page 1-12

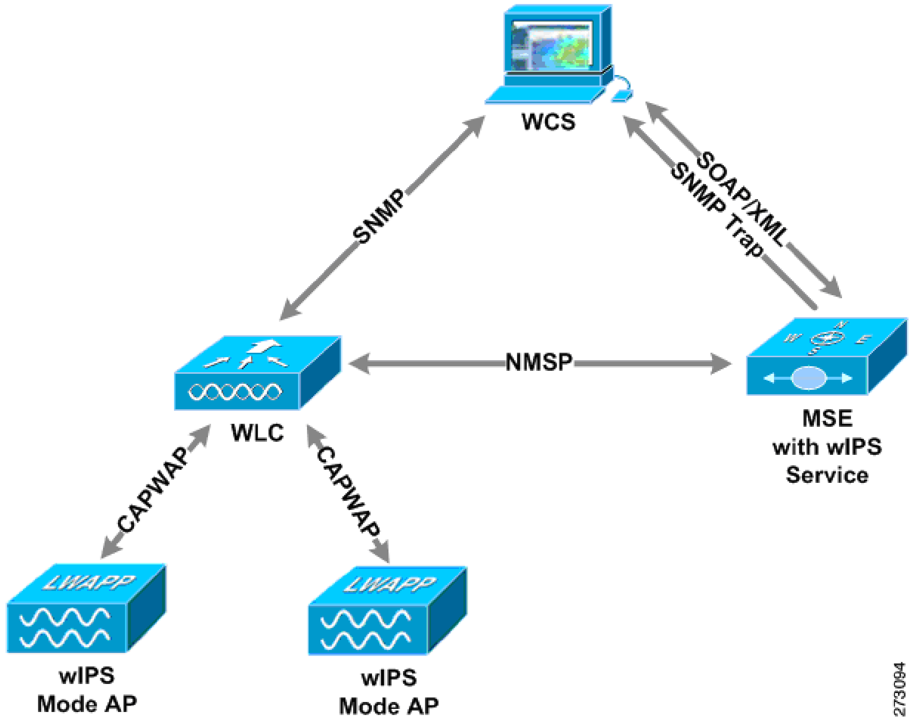
Overview of wIPS

Cisco Adaptive Wireless Intrusion Prevention System (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.

Built on Cisco Unified Wireless Network (CUWN) and leveraging the efficiencies of Cisco Motion, wIPS is deployment-hardened and enterprise-ready. Cisco's wIPS is made up of the following components that work together to provide a unified security monitoring solution.

- A 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.
- An 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.
- Wireless 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. WCS is also used to view wIPS alarms, forensics, reporting, and to access the attack encyclopedia.

Figure 1-1 Wireless Intrusion Prevention System



Communication among the system components involves the following protocols:

- Control and Provisioning of Wireless Access Points (CAPWAP)–This protocol is the successor to LWAPP and is used for communication between access points and controllers. It provides a bi-directional tunnel in which alarm information is sent to the controller and configuration information is sent to the access point.
- Network Mobility Services Protocol (NMSP)–The protocol handles communication between controllers and the mobility services engine. In an wIPS deployment, this protocol provides a pathway for alarm information to be aggregated from controllers and forwarded to the mobility services engine and for wIPS configuration information to be pushed to the controller. This protocol is encrypted.
  - Controller TCP Port: 16113
- Simple Object Access Protocol (SOAP/XML)–The method of communication between the mobility services engine and WCS. This protocol is used to distribute configuration parameters to the wIPS service running on the mobility services engine.
  - MSE TCP Port: 443
- Simple Network Management Protocol (SNMP)–This protocol is used to forward wIPS alarm information from the mobility services engine to the WCS. It is also employed to communicate rogue access point information from the controller to WCS.

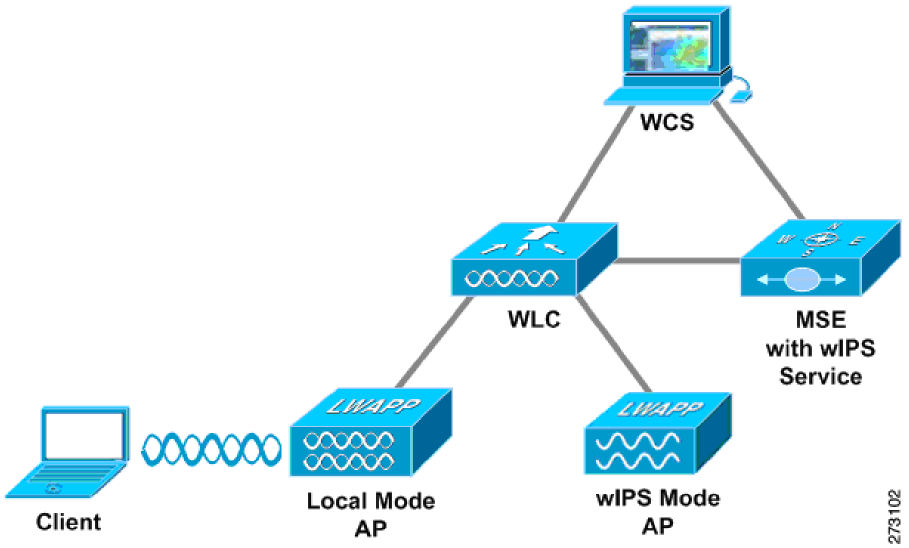
wIPS in a Cisco Unified Wireless Network

You can integrate wIPS within the CUWN infrastructure or overlay wIPS on the CUWN or Cisco autonomous wireless network (or third party wireless network). A summary of each deployment and its uses is summarized in this section.

wIPS Integrated Within a Cisco Unified Wireless Network

An integrated wIPS deployment is a system design in which both *local* mode and wIPS *monitor mode* access points are intermixed on the same controller, and managed by the same Cisco WCS. Cisco recommends this configuration as it allows the tightest integration between the client serving and monitoring infrastructure (Figure 1-2).

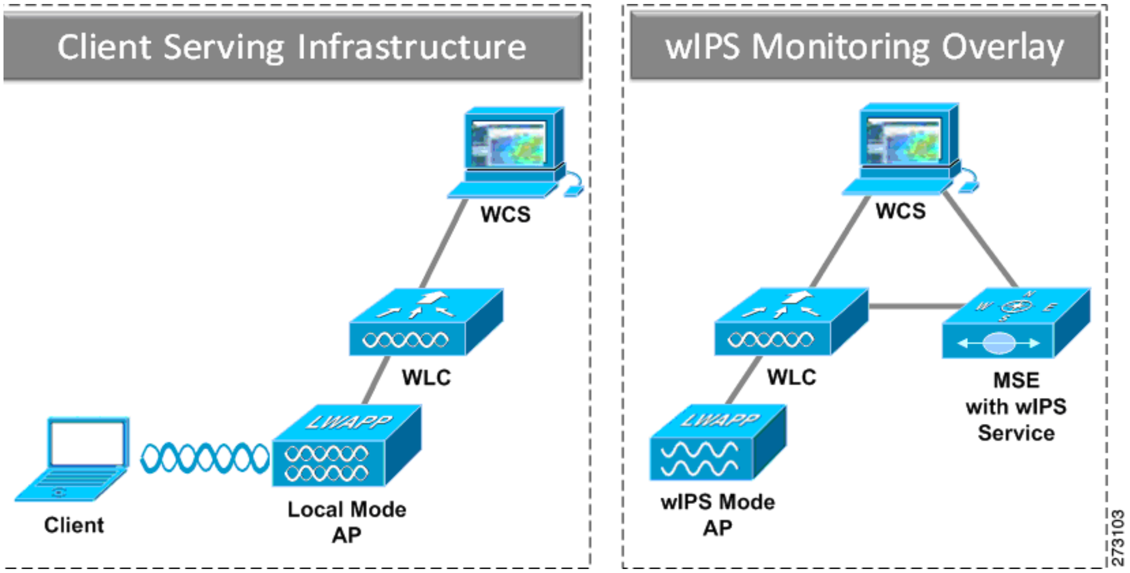
Figure 1-2 wIPS Integrated Within CUWN



wIPS Overlay Deployment in a Cisco Unified Wireless Network

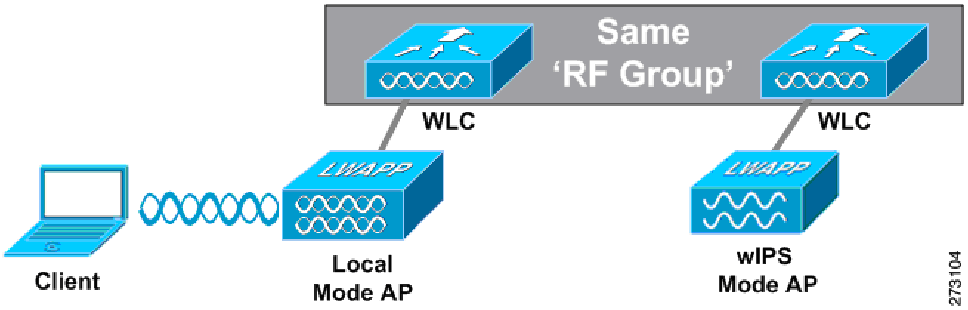
In a wIPS Overlay deployment, the wIPS monitoring infrastructure is completely separate from the client serving infrastructure. Each distinct system has its own set of controllers, access points and Cisco WCS. The reason for selecting this deployment model often stems from business mandates that require distinct network infrastructure and security infrastructure systems with separate management consoles (Figure 1-3). This deployment model is also used when the total number of access points (wIPS monitor and local mode) exceed the 3000 access point limit contained in WCS.

Figure 1-3 wIPS Overlay Monitoring Network Deployment in CUWN



In order to configure the wIPS Overlay Monitoring network to provide security assessment of the client serving infrastructure, specific configuration items must be completed. The wIPS system operates on the assumption that only attacks against trusted devices must be logged. In order for an overlay system to view a separate Cisco Unified WLAN infrastructure as trusted, the controllers must be in the same RF Group (Figure 1-4).

Figure 1-4 Controllers in Same RF Group for wIPS Overlay Deployment



As a result of separating the client serving infrastructure from the wIPS monitoring overlay infrastructure, several monitoring caveats arise:

- wIPS alarms are only shown on the wIPS Overlay WCS instance
- Management Frame Protection (MFP) alarms are only shown on the client infrastructure WCS instance
- Rogue alarms are shown in both WCS instances
- Rogue location accuracy is greater on the client serving infrastructure Cisco WCS because this deployment employs a greater density of access points than the wIPS overlay deployment
- Over-the-air rogue mitigation is more scalable in an integrated wIPS model, as the local-mode access points are employed in mitigation actions
- The security monitoring dashboard is incomplete on both Cisco WCS instances because some events such as wIPS only exist on the wIPS Overlay WCS
  - To monitor the comprehensive security of the wireless network, both security dashboard instances must be observed

Table 1-1 summarizes some of the key differences between client serving and overlay deployments.

Table 1-1 wIPS Client Serving and wIPS Monitoring Overlay Comparison

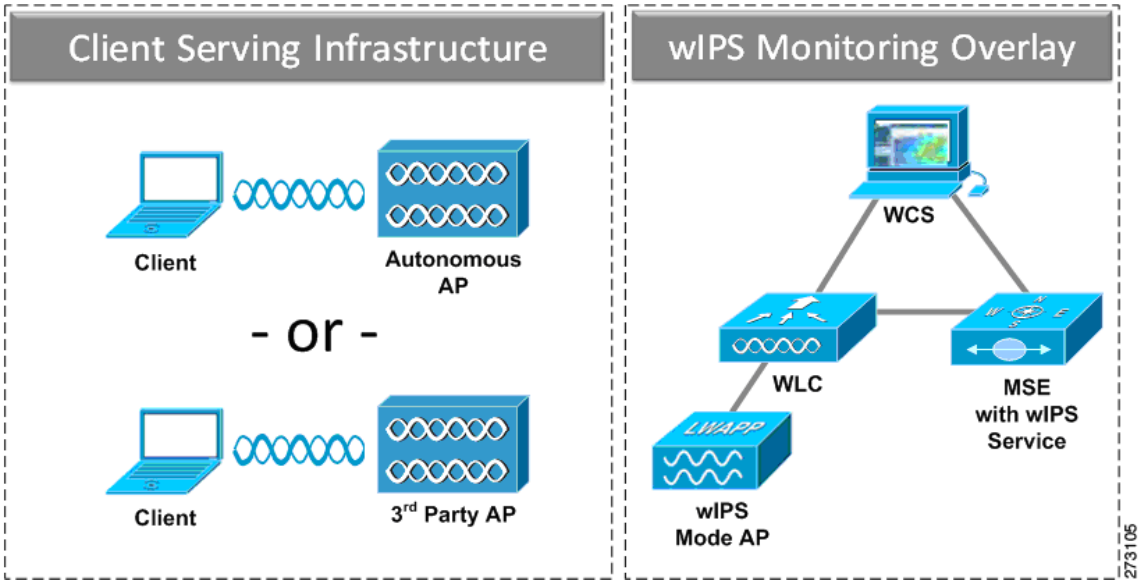
	Client Serving Infrastructure WCS	**wIPS Monitoring Overlay WCS**
wIPS alarms	No	Yes
MFP alarms	Yes	No
Rogue alarms	Yes	Yes
Rogue location	High accuracy	Low accuracy
Rogue containment	Yes	Yes, but scalable

One challenge of the overlay solution is the possibility of lightweight access points on either the client serving infrastructure or wIPS monitoring overlay associating to the wrong controller. Association with the wrong controller can be addressed by specifying the primary, secondary and tertiary controller names for each access point (both local and wIPS monitor mode). In addition, Cisco recommends that the controllers for each respective solution have separate management VLANs for communication with their respective access points and that access control lists (ACLs) are used to prevent CAPWAP traffic from crossing these VLAN boundaries.

wIPS Overlay in Autonomous or Other Wireless Network

The Adaptive wIPS solution is also capable of performing security monitoring over an existing WLAN infrastructure other than CUWN. In this case, the client serving infrastructure is completely separate and uncoordinated with the wIPS overlay. The application for this deployment is security monitoring of either Cisco autonomous access points or third-party access points (Figure 1-5).

Figure 1-5 wIPS Overlay in Autonomous



Differences Between Controller IDS and Adaptive wIPS

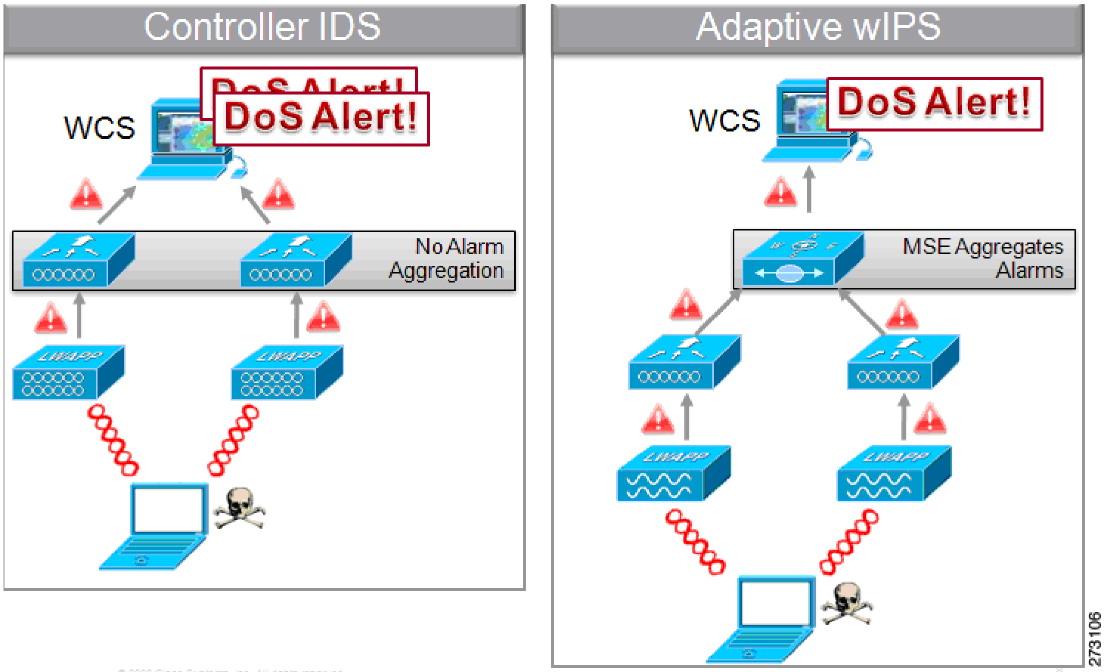
Reduction in False Positives

Cisco wIPS facilitates a reduction in false positives with respect to security monitoring of the wireless network. In contrast to Cisco's controller-based solution, which triggers an alarm when it detects a number of management frames over the air, wIPS only triggers an alarm when it detects a number of management frames over the air that are causing damage to the wireless infrastructure network. This a result of the wIPS system being able to dynamically identify the state and validity of access points and clients present in the wireless infrastructure. Only when attacks are launched against the infrastructure are alarms raised.

Alarm Aggregation

One major differentiation between Cisco's existing controller-based IDS system and its wIPS system is the unique attacks seen over the air are correlated and aggregated into a single alarm. This is accomplished by the wIPS system automatically assigning a unique hash key to each particular attack the first time it is identified. If the attack is received by multiple wIPS access points, it will only be forwarded to the WCS once because alarm aggregation takes place on the mobility services engine. The existing controller-based IDS system does not aggregate alarms (Figure 1-6).

Figure 1-6 Alarm Aggregation Using Cisco's Controller-based IDS versus Adaptive wIPS



Another major differentiation between the controller-based IDS and wIPS is the number of attacks that each system can detect. As described in the sub-sections and showcased in the tables below, wIPS can detect a multitude of attacks and attack tools. These attacks include both denial of service (DoS) attacks and security penetration attacks.

DoS Attacks

A DoS attack involves mechanisms which are designed to prohibit or slow successful communication within a wireless network. These often incorporate a number of spoofed frames which are designed to drop or falter legitimate connections within the wireless network. Although a DoS attack can be devastating to a wireless networks ability to deliver reliable services, they do not result in a data breach and their negative consequences are often over once the attack has stopped. Table 1-2 compares the DoS attacks detected by the controller-based IDS and wIPS service.

Table 1-2 DoS Attack Detection By Controller IDS and wIPS

Alarm Name	Detected by Controller IDS	Detected by wIPS
Association flood	X	X
Association table overflow		X
Authentication flood	X	X
EAPOL-Start attack	X	X
PS-Poll flood		X
Unauthenticated Association		X
CTS Flood		X
Queensland University of Technology Exploit		X
RF jamming attack		X
RTS flood		X
Virtual carrier attack	X	X
Authentication-failure attack		X
Deauthentication broadcast attack	X	X
Deauthentication flood attack	X	X
Disassociation broadcast attack		X
Disassociation flood attack	X	X
EAPOL-logoff attack	X	X
FATA-jack tool detected		X
Premature EAP-failure attack		X
Premature EAP-success attack		X

Security Penetration Attacks

Arguably the more harmful of the two attack types threatening wireless networks, a security penetration is designed to capture or expose information such as sensitive data or encryption keys that can later be used for exposing confidential data. A security penetration attack can involve targeted queries against the infrastructure or replay attacks that aim to break cryptographic keys. Security Penetration attacks can also be harmful to the client by which an attempt to lure the client onto a fake access point such as a Honeypot. Table 1-3 compares the security penetration attacks detected by the controller-based IDS and wIPS service.

Table 1-3 Security Penetration Attack Detection By Controller IDS and wIPS

Alarm Name	Detected by Controller IDS	Detected by wIPS
Airsnarf attack		X
ChopChop Attack		X
Day-zero attack by WLAN security anomaly		X
Day-zero attack by device security anomaly		X

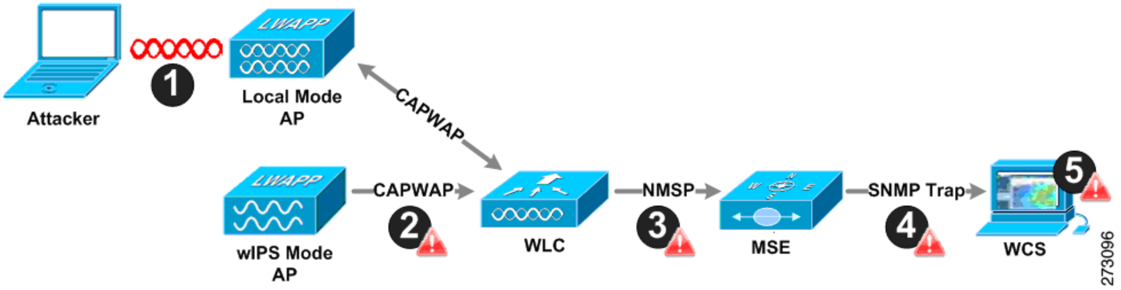
Table 1-3 Security Penetration Attack Detection By Controller IDS and wIPS (continued)

Alarm Name	Detected by Controller IDS	Detected by wIPS
Device probing for access points		X
Dictionary attack on EAP methods		X
EAP attack against 802.1x authentication		X
Fake access points detected	X	X
Fake DHCP server detected		X
Fast WEP crack detected		X
Fragmentation Attack		X
Hotspotter tool detected		X
Malformed 802.11 packets detected		X
Man in the middle attack detected		X
NetStumbler detected	X	X
PSPF violation		X
ASLEAP attack detected		X
Honey pot access point detected	X	X
Soft access point or Host access point detected		X
Spoofed MAC address detected		X
Suspicious after-hours traffic		X
Unauthorized association by vendor list		X
Unauthorized association detected		X
Wellenreiter detected	X	X

wIPS Alarm Flow

The Adaptive wIPS system follows a linear chain of communication to propagate attack information obtained from initially scanning the airwaves to forwarding information to Cisco WCS.

Figure 1-7 Alarm Flow Within Network



1. In order for an alarm to be triggered on the wIPS system, an attack must be launched against a legitimate access point or client. Legitimate access points and clients are discovered automatically in a CUWN by trusting devices broadcasting the same RF-Group name. In this configuration, the

system dynamically maintains a list of local-mode access points and their associated clients. The system can also be configured to trust devices by SSID using the SSID Groups feature. Only attacks which are considered harmful to the WLAN infrastructure are propagated upwards to the rest of the system.

2. Once an attack is identified by the wIPS monitor mode access point, an alarm update is sent to the controller and is encapsulated inside the CAPWAP control tunnel.
3. The controller transparently forwards the alarm update from the access point to the wIPS service running on the mobility services engine. The protocol used for this communication is Network Mobility Service Protocol (NMSP).
4. Once received by the wIPS service on the mobility services engine, the alarm update is added to the alarm database for archival and attack tracking. An SNMP trap is forwarded to WCS. The SNMP trap contains the attack information. If multiple alarm updates are received referencing the same attack (for example, if multiple access points hear the same attack) only one SNMP trap is sent to WCS.
5. The SNMP trap containing the alarm information is received and displayed by WCS.

Forensics

Cisco's Adaptive wIPS system provides the ability to capture attack forensics for further investigation and troubleshooting purposes. At a base level, the forensics capability is a toggle-based packet capture facility which logs and retrieves a set of wireless frames. This feature is enabled on a per attack basis within a wIPS profile. wIPS profiles are configured on WCS.

Once enabled, the forensics feature is triggered when a specific attack alarm is seen over the airwaves. The forensic file created is based on the packets contained within the buffer of the wIPS monitor mode access point that triggered the original alarm. This file is transferred to the controller via CAPWAP, which then forwards the forensic file via NMSP to wIPS running on the mobility services engine. The file is stored within the forensic archive on the mobility services engine until the user configured disk space limit for forensics is reached. By default, this limit is 20 Gigabytes, which when reached, causes the oldest forensic files to be removed. Access to the forensic file is obtained by opening the alarm in WCS which contains a hyperlink to the forensic file. The files are stored in a *.CAP* file format which is accessed by either WildPacket *Omnipeek*, AirMagnet *WiFi Analyzer*, *Wireshark* or any other packet capture program which supports this format. Wireshark is available at http://www.wireshark.org.

Note Cisco recommends that the forensics capability of wIPS system be used sparingly and disabled after the desired information is captured. This primarily because it places an intensive load on the access point as well as interrupts scheduled channel scanning. A wIPS access point cannot simultaneously perform channel scanning and produce a forensic file. While the forensic file is being dumped, channel scanning is delayed.

Rogue Detection

An access point in wIPS-optimized monitor mode performs rogue threat assessment and mitigation using the same logic as current CUWN implementations. This allows a wIPS mode access point to scan, detect and contain rogue access points and ad-hoc networks. Once discovered, this information regarding rogue wireless devices is reported to WCS where rogue alarm aggregation takes place.

However, with this functionality comes the caveat that if a containment attack is launched using a wIPS mode access point, its ability to perform methodical attack-focused channel scanning is interrupted for the duration of the containment.

Anomaly Detection

wIPS includes specific alarms pertaining to anomalies in attack patterns or device characteristics captured. The anomaly detection system takes into account the historic attack log and device history contained within the mobility services engine to baseline the typical characteristics of the wireless network. The anomaly detection engine is triggered when events or attacks on the system undergo a measurable change as compared to historical data kept on the mobility services engine. For example, if the system regularly captures a few MAC spoofing events each day, and then on another day MAC spoofing events are up 200%, an anomaly alarm is triggered on the mobility services engine. This alarm is then sent to WCS to inform the administrator that something else is going on in the wireless network beyond traditional attacks that they system may encounter. The anomaly detection alarm can also be employed to detect day-zero attacks that might not have a preexisting signature in the wIPS system.

Default Configuration Profiles

To simplify the configuration tuning for each specific WLAN security deployment, wIPS includes a number of default profiles tailored to meet the security needs of specific industries or deployments. The templates summarize the differing risk profiles and requirements for security monitoring of varying deployments. The specific profiles include Education, Enterprise (Best), Enterprise (Rogue), Financial, Healthcare, Hotspot (Open Security), Hotspot (802.1x Security), Military, Retail, Tradeshow, and Warehouse. The profiles can be further customized to address the specific needs of the prospective deployment.

Integration into Release 6.0 Features

wIPS tightly integrates into an existing CUWN to leverage the security features introduced in previous releases. On the security dashboard, wIPS events display under their own category.

Configuration Guide Overview

This configuration guide addresses the configuration of wIPS and mobility services engine. A summary of the configuration items is noted below.

Adding and Deleting Mobility Services Engine

You can use Cisco WCS to add and delete mobility services engine within the network. You are also able to define the service supported on the mobility services engine. Refer to Chapter 2, "Adding and Deleting Systems" for configuration details.

Editing Mobility Services Engine Properties

You can use Cisco WCS to configure the following parameters on the mobility services engine. Refer to Chapter 4, "Configuring and Viewing System Properties" for configuration details.

- General Properties: Enables you to assign a contact name, username, password, and HTTP for the mobility services engine.
- NMSP Parameters: Enables you to modify Network Mobility Services Protocol (NMSP) parameters such as echo and neighbor dead intervals as well as response and retransmit periods. NMSP is the protocol that manages communication between the mobility services engine and the controller.
- Active Sessions: Enables you to view active user sessions on the mobility services engine.
- Trap Destinations: Enables you to specify which Cisco WCS 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.
- Advanced Parameters: 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.

Managing Users and Groups

You can use Cisco WCS to add, delete, and edit user session and user group parameters as well as add and delete host access records. Refer to Chapter 5, "Managing Users and Groups" for configuration details.

Mobility Services Engine Synchronization

Cisco WCS pushes wIPS information to the mobility services engine to maintain accurate information between the mobility services engine and controller. Cisco WCS provides you with two ways to synchronize: manual and automatic (auto-sync). Refer to Chapter 3, "Synchronizing Mobility Services Engines" for specifics.

Configuring wIPS and Profile Management

You can use Cisco WCS to configure the Cisco Adaptive wIPS service.

Refer to Chapter 6, "Configuring wIPS and Profiles" for specifics.

Monitoring Capability

You can use Cisco WCS to monitor alarms, events, and logs generated by mobility services engine. You can also monitor the status of mobility services engines, clients, and tagged assets. Additionally, you can generate a utilization report for the mobility services engine to determine CPU and memory utilization as well as counts for clients, tags and rogue access points and clients. Refer to Chapter 7, "Monitoring the System and Services" for specifics.

Maintenance Operations

You can use Cisco WCS to recover a password, back up mobility services engine data to a predefined FTP folder on Cisco WCS at defined intervals, and restore the mobility services engine data from that Cisco WCS. Other mobility services engine maintenance operations that you can perform include: downloading new software images to all associated mobility services engines from any Cisco WCS station, defragmenting the mobility services engine database, restarting a mobility services engine, shutting down a mobility services engine and clearing mobility services engine configurations. Refer to Chapter 8, "Performing Maintenance Operations" for specifics.

System Compatibility

Note Refer to the *Cisco 3300 Mobility Services Engine Release Note* for the latest system (controller, WCS, mobility services engine) compatibility information, feature support, and operational notes for your current release at: http://www.cisco.com/en/US/products/ps9742/prod_release_notes_list.html

CHAPTER 2

Adding and Deleting Systems

This chapter describes how to add and delete a mobility services engine from Cisco WCS.

This chapter contains the following sections:

Adding a Mobility Services Engine to Cisco WCS

To add a Cisco 3300 Series Mobility Services Engine to Cisco WCS, log into WCS and follow these steps:

Step 1 Verify that you can ping the mobility service engine that you want to add from Cisco WCS.

Step 2 Choose **Services > Mobility Services** to display the Mobility Services window.

Step 3 From the Select a command drop-down menu, choose **Add Mobility Services Engine** and click **Go**.

Step 4 In the Device Name field, enter a name for the mobility services engine.

Step 5 In the IP Address field, enter the mobility services engine's IP address.

Step 6 (Optional) In the Contact Name field, enter the name of the mobility services engine administrator.

Step 7 In the User Name and Password fields, enter the username and password for the mobility services engine.

The default username and password are both *admin*.

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, Cisco strongly recommends that you rerun the automatic installation script and change the username and password.

Step 8 Click **Next**. The Select Mobility Service window appears.

Step 9 To enable a service on the mobility services engine, check the check box next to that service.

Note A mobility services engine can support multiple services.

Step 10 Click **Save**.

Note After adding a new mobility services engine, you can synchronize network designs (campus, building, and outdoor maps), controllers, switches (Catalyst Series 3000 only), and event groups on the local mobility services engine using Cisco WCS. You can do this synchronization immediately after adding a new mobility services engine or at a later time. To synchronize the local and Cisco WCS databases, refer to Chapter 3.

Deleting a Mobility Services Engine from the Cisco WCS

To delete a mobility services engine from the Cisco WCS database, follow these steps:

Step 1 Click **Services > Mobility Services** to display the Mobility Services window.

Step 2 Select the mobility services engine(s) to be deleted by checking the corresponding check box(es).

Step 3 From the Select a command drop-down menu, select **Delete Service(s)** and click **Go**.

Step 4 Click **OK** to confirm that you want to delete the selected mobility services engine from the WCS database.

Step 5 Click **Cancel** to stop deletion.

Registering Client and wIPS 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 emailed to you after successfully registering a PAK.

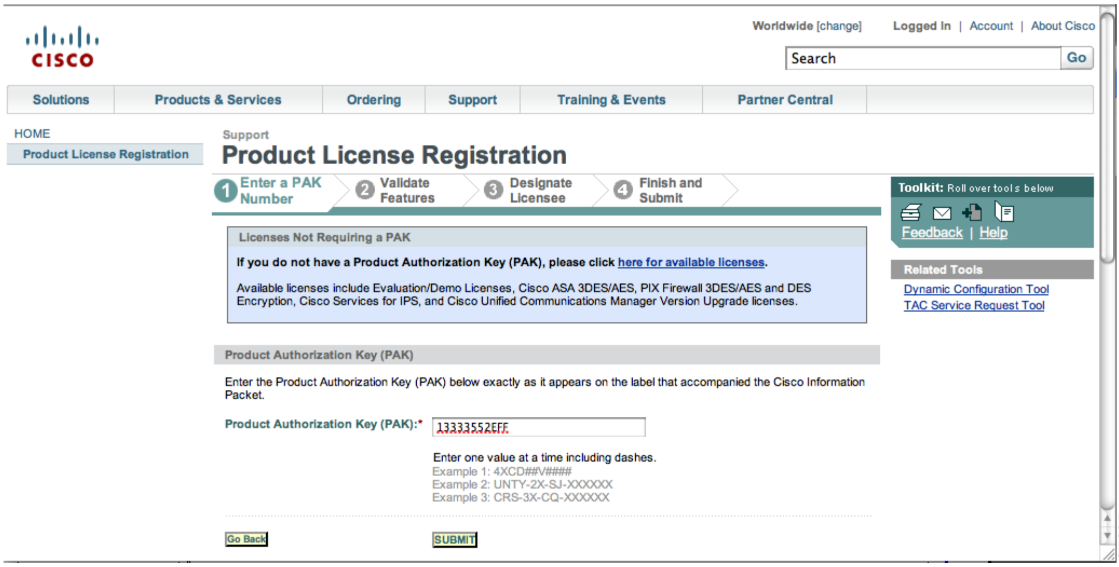
Client and wIPS PAKs are registered with Cisco.

Note Tag PAKs are registered with AeroScout. Refer to the Cisco Context-Aware Serve Configuration Guide: http://www.cisco.com/en/US/products/ps9806/products_installation_and_configuration_guides_list.html

To register a product authorization key (PAK) to obtain a license file for install, follow these steps:

Step 1 Open a browser window and enter www.cisco.com/go/license. Enter the PAK and click **SUBMIT** (see Figure 2-1).

Figure 2-1 Enter PAK Number Window



Product License Registration

Licenses Not Requiring a PAK

If you do not have a Product Authorization Key (PAK), please click here for available licenses.

Available licenses include Evaluation/Demo Licenses, Cisco ASA 3DES/AES, PIX Firewall 3DES/AES and DES Encryption, Cisco Services for IPS, and Cisco Unified Communications Manager Version Upgrade licenses.

Product Authorization Key (PAK)

Enter the Product Authorization Key (PAK) below exactly as it appears on the label that accompanied the Cisco Information Packet.

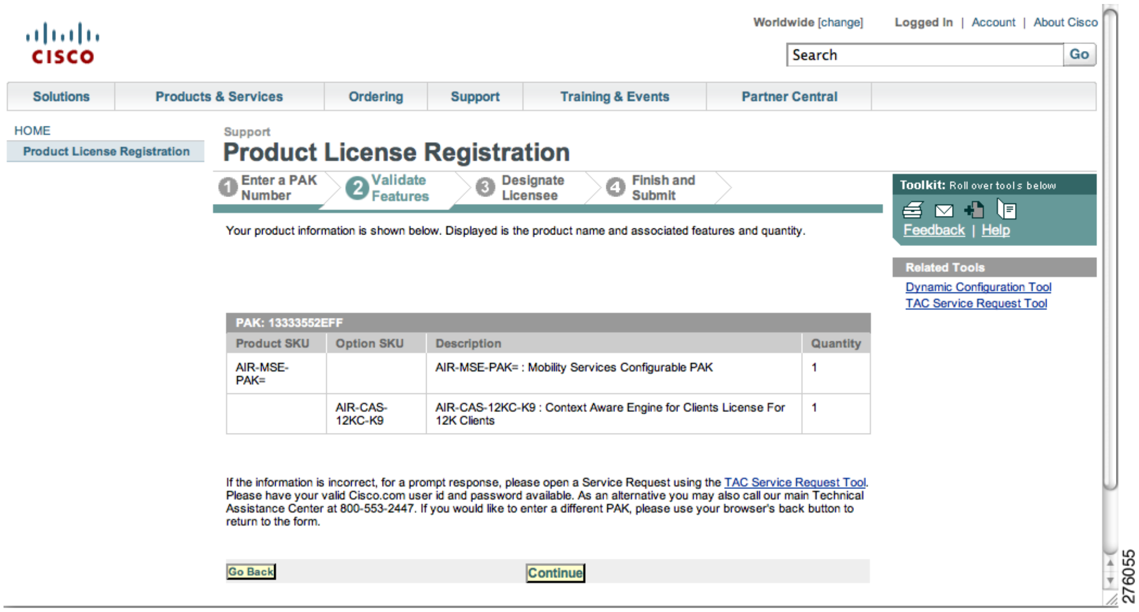
Product Authorization Key (PAK):* 13333552EFF

Enter one value at a time including dashes.
Example 1: 4XCD##V####
Example 2: UNTY-2X-SJ-XXXXXX
Example 3: CRS-3X-CQ-XXXXXX

Step 2 Verify the license purchase. Click **Continue** if correct (see Figure 2-2). The licensee entry window appears (see Figure 2-3).

Note If the license is incorrect, click **TAC Service Request Tool** link (right) to report the problem.

Figure 2-2 Validate License Purchase Window



Support

Product License Registration

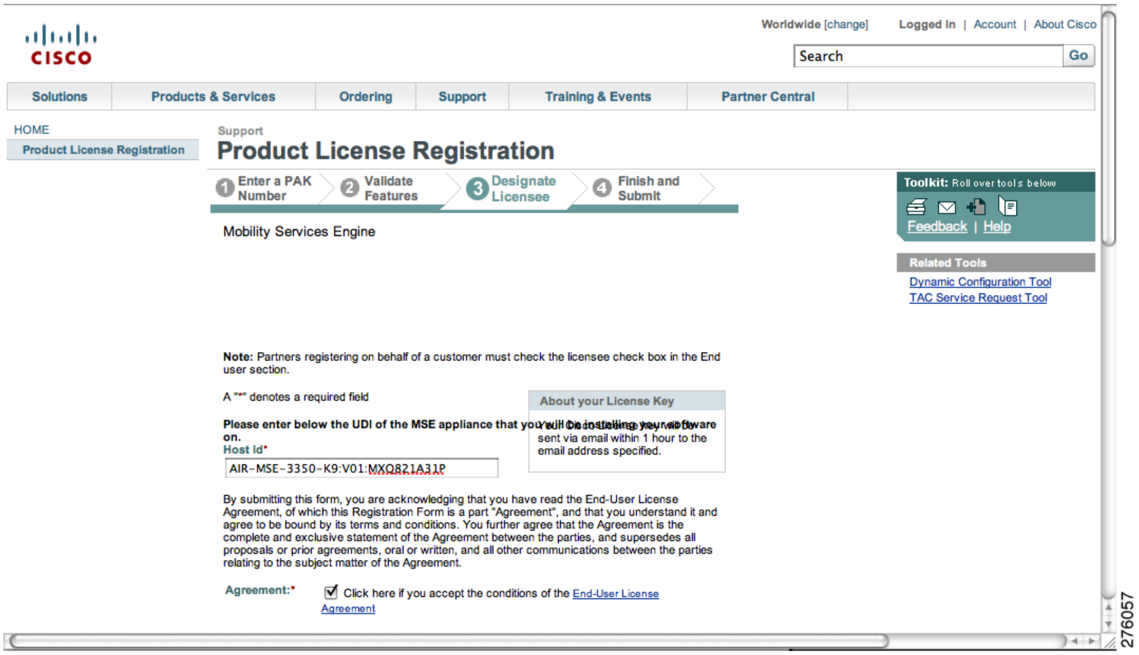
Your product information is shown below. Displayed is the product name and associated features and quantity.

PAK: 13333552EFF

Product SKU	Option SKU	Description	Quantity
AIR-MSE-PAK=		AIR-MSE-PAK= : Mobility Services Configurable PAK	1
	AIR-CAS-12KC-K9	AIR-CAS-12KC-K9 : Context Aware Engine for Clients License For 12K Clients	1

If the information is incorrect, for a prompt response, please open a Service Request using the TAC Service Request Tool. Please have your valid Cisco.com user id and password available. As an alternative you may also call our main Technical Assistance Center at 800-553-2447. If you would like to enter a different PAK, please use your browser's back button to return to the form.

Figure 2-3 Designate Licensee Window, 1 of 2



Support

Product License Registration

Mobility Services Engine

Note: Partners registering on behalf of a customer must check the licensee check box in the End user section.

A "*" denotes a required field

Please enter below the UDI of the MSE appliance that you will be installing your software on.

Host Id*: AIR-MSE-3350-K9:V01:MXQ821A31P

About your License Key

Your Cisco License Key will be sent via email within 1 hour to the email address specified.

By submitting this form, you are acknowledging that you have read the End-User License Agreement, of which this Registration Form is a part "Agreement", and that you understand it and agree to be bound by its terms and conditions. You further agree that the Agreement is the complete and exclusive statement of the Agreement between the parties, and supersedes all proposals or prior agreements, oral or written, and all other communications between the parties relating to the subject matter of the Agreement.

Agreement:* ☑ Click here if you accept the conditions of the End-User License Agreement

Step 3 At the Designate Licensee window:

a. Enter the mobility service engine's UDI in the host ID field. This is the mobility services engine on which the license will be installed.

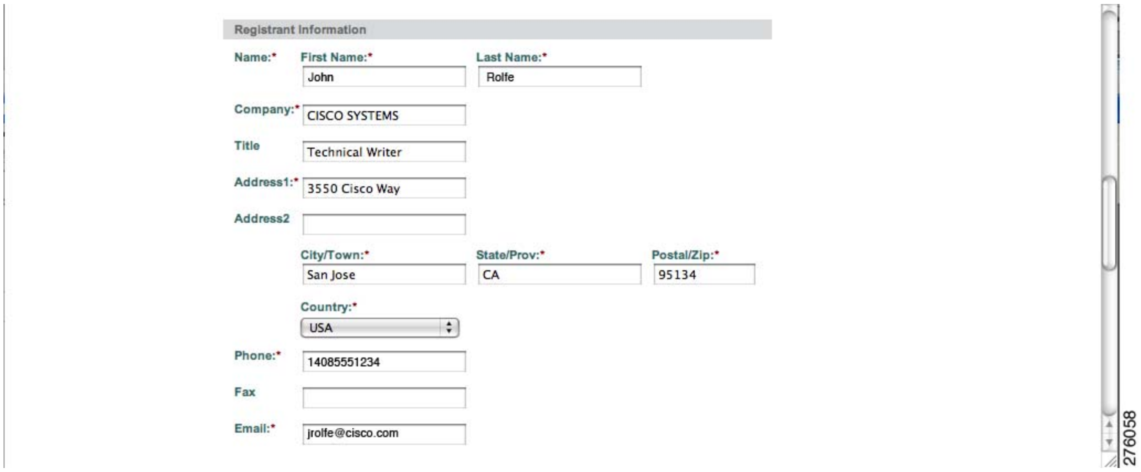
Note UDI information for a mobility services engine is found on the General Properties panel at Services > Mobility Services Engine > *Device Name* > *System*.

b. Check **Agreement** check box. Registrant information appears beneath the Agreement check box (see Figure 2-4).

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.

Figure 2-4 Designate Licensee Window, 2 of 2



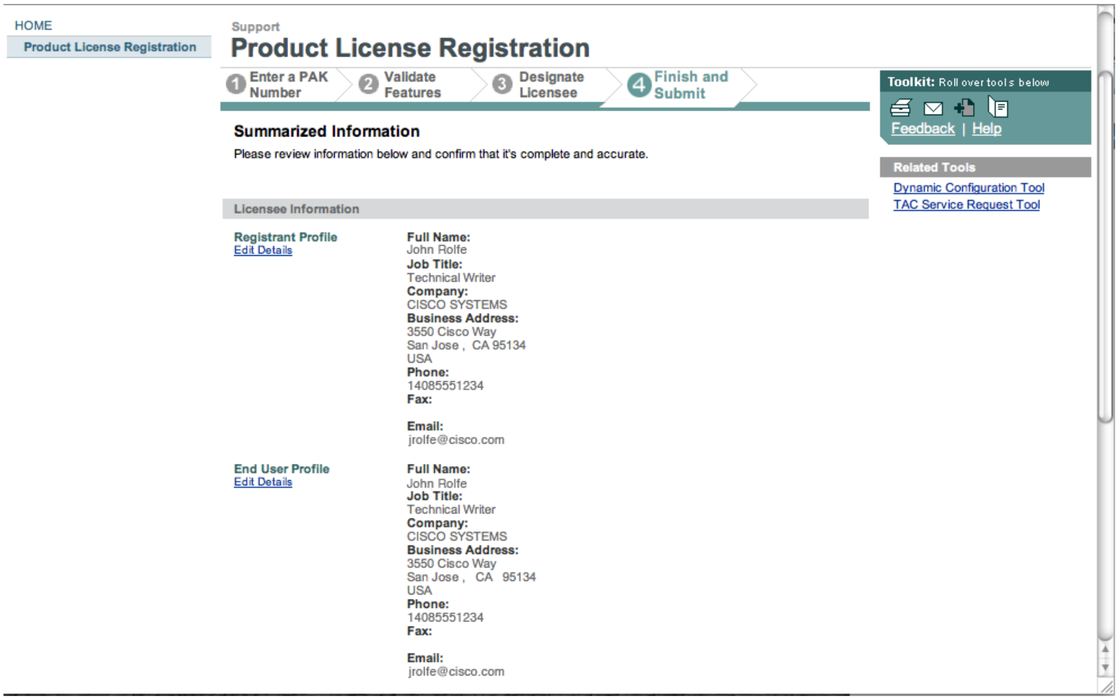
Registrant Information

Name:*	First Name:* John	Last Name:* Rolfe	
Company:*	CISCO SYSTEMS		
Title	Technical Writer		
Address1:*	3550 Cisco Way		
Address2			
	City/Town:* San Jose	State/Prov:* CA	Postal/Zip:* 95134
	Country:* USA		
Phone:*	14085551234		
Fax			
Email:*	jrolfe@cisco.com		

c. If registrant and end user are not the same person, check **Licensee (End-User)** check box beneath registrant information and enter the end user's information.

d. Click **Continue**. A summary of entered data appears (see Figure 2-5).

Figure 2-5 Finish and Submit Window



Summarized Information

Please review information below and confirm that it's complete and accurate.

Licensee Information

Registrant Profile
Edit Details

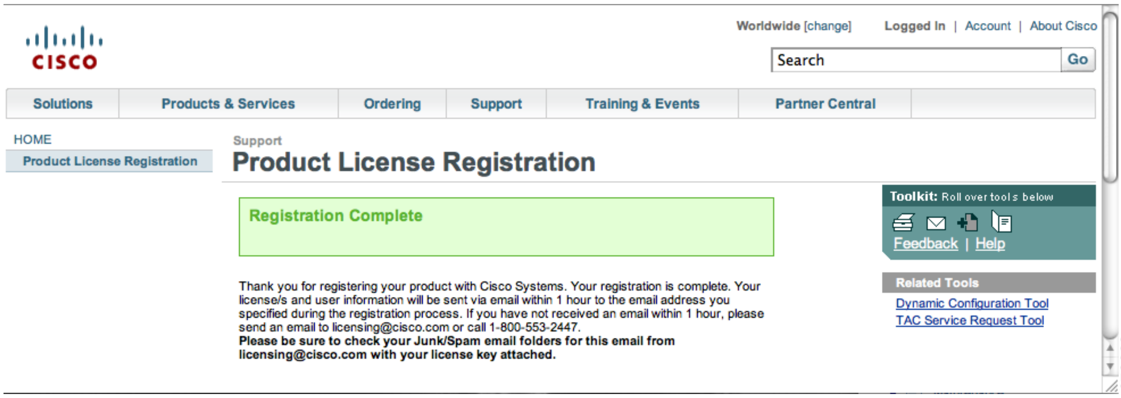
Full Name: John Rolfe
Job Title: Technical Writer
Company: CISCO SYSTEMS
Business Address:
3550 Cisco Way
San Jose , CA 95134
USA
Phone: 14085551234
Fax:
Email: jrolfe@cisco.com

End User Profile
Edit Details

Full Name: John Rolfe
Job Title: Technical Writer
Company: CISCO SYSTEMS
Business Address:
3550 Cisco Way
San Jose , CA 95134
USA
Phone: 14085551234
Fax:
Email: jrolfe@cisco.com

Step 4 At the Finish and Submit window, review registrant and end user data. Click **Edit Details** to correct information. Click **Submit**. A confirmation window appears (see Figure 2-6).

Figure 2-6 Registration Confirmation Window



Registration Complete

Thank you for registering your product with Cisco Systems. Your registration is complete. Your license/s and user information will be sent via email within 1 hour to the email address you specified during the registration process. If you have not received an email within 1 hour, please send an email to licensing@cisco.com or call 1-800-553-2447.
Please be sure to check your Junk/Spam email folders for this email from licensing@cisco.com with your license key attached.

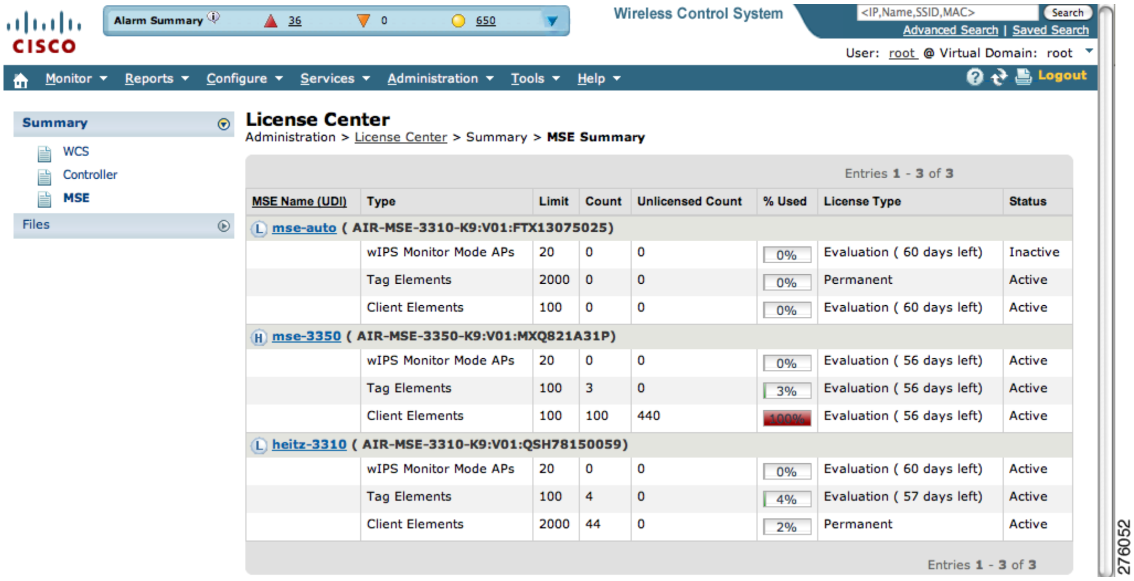
Installing wIPS License Files

You can install client and wIPS licenses from Cisco WCS.

To add a client or wIPS license to Cisco WCS after registering the PAK, follow these steps:

Step 1 Choose **Administration > License Center** (see Figure 2-7).

Figure 2-7 Administration > License Center Window



License Center

Administration > License Center > Summary > **MSE Summary**

Entries 1 - 3 of 3

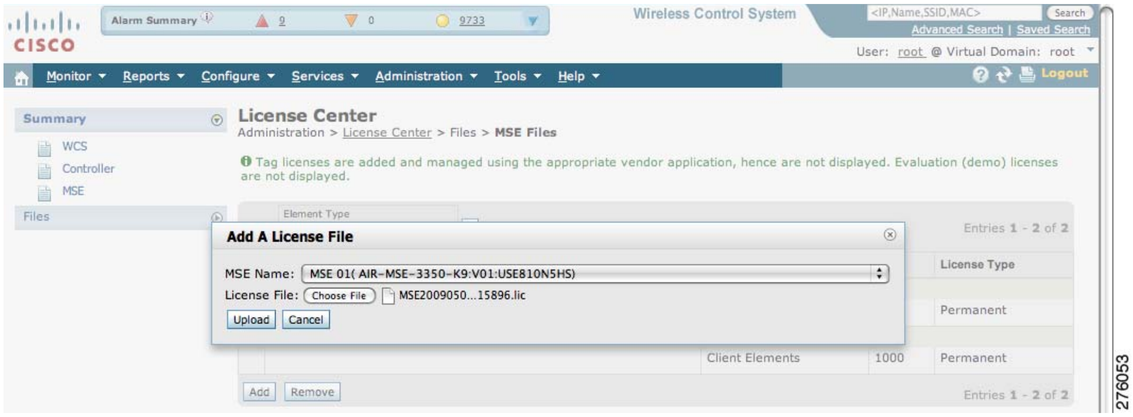
MSE Name (UDI)	Type	Limit	Count	Unlicensed Count	% Used	License Type	Status
mse-auto (AIR-MSE-3310-K9:V01:FTX13075025)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (60 days left)	Inactive
	Tag Elements	2000	0	0	0%	Permanent	Active
	Client Elements	100	0	0	0%	Evaluation (60 days left)	Active
mse-3350 (AIR-MSE-3350-K9:V01:MXQ821A31P)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (56 days left)	Active
	Tag Elements	100	3	0	3%	Evaluation (56 days left)	Active
	Client Elements	100	100	440	100%	Evaluation (56 days left)	Active
heitz-3310 (AIR-MSE-3310-K9:V01:QSH78150059)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (60 days left)	Active
	Tag Elements	100	4	0	4%	Evaluation (57 days left)	Active
	Client Elements	2000	44	0	2%	Permanent	Active

Entries 1 - 3 of 3

Step 2 Choose **Files > MSE Files** (left panel).

Step 3 Click **Add**. A pop-up entry panel appears (see Figure 2-8).

Figure 2-8 Add a License File Panel



License Center

Administration > License Center > Files > **MSE Files**

Tag licenses are added and managed using the appropriate vendor application, hence are not displayed. Evaluation (demo) licenses are not displayed.

Add A License File

MSE Name: MSE 01(AIR-MSE-3350-K9:V01:USE810N5HS)

License File: Choose File MSE2009050...15896.lic

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**. Newly added license appears in MSE license file list.

CHAPTER 3

Synchronizing Mobility Services Engines

This chapter describes how to synchronize Cisco wireless LAN controllers and Cisco WCS with mobility services engines.

This chapter contains the following sections:

Synchronizing Cisco WCS and Mobility Services Engines

This section describes how to synchronize Cisco WCS and mobility services engines manually and automatically.

After adding a mobility services engine to Cisco WCS, you can synchronize network designs (campus, building, and outdoor maps), controllers (name and IP address), specific Catalyst Series 3000 and 4000 switches, and event groups with the mobility services engine.

- Network Design—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.
- Controller—is a selected controller that is associated and regularly exchanges location information with a mobility services engine. Regular synchronization ensures location accuracy.
- Switches (wired)—are 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 4000 series: 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
- Event Groups—are a group of predefined events that define triggers that generate an event. Regular synchronization ensures that the latest defined events are tracked.

Note Be sure to verify software compatibility between the controller, Cisco WCS, and the mobility services engine before synchronizing. Refer to the latest mobility services engine release note at the following link: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

Note Communication between the mobility services engine and Cisco WCS and the controller is in universal time code (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 WCS server. An NTP server is required to automatically synchronize time between the controller, Cisco WCS, and the mobility services engine.

To synchronize Cisco WCS network designs, a controller, or event groups with the mobility services engine, follow these steps:

Step 1 Choose **Services > Synchronize Services** to display the Mobility Services > Synchronize WCS and MSE(s) window.

A four-tabbed window appears with the following headings: Network Designs, Controllers, Switches, and Event Groups.

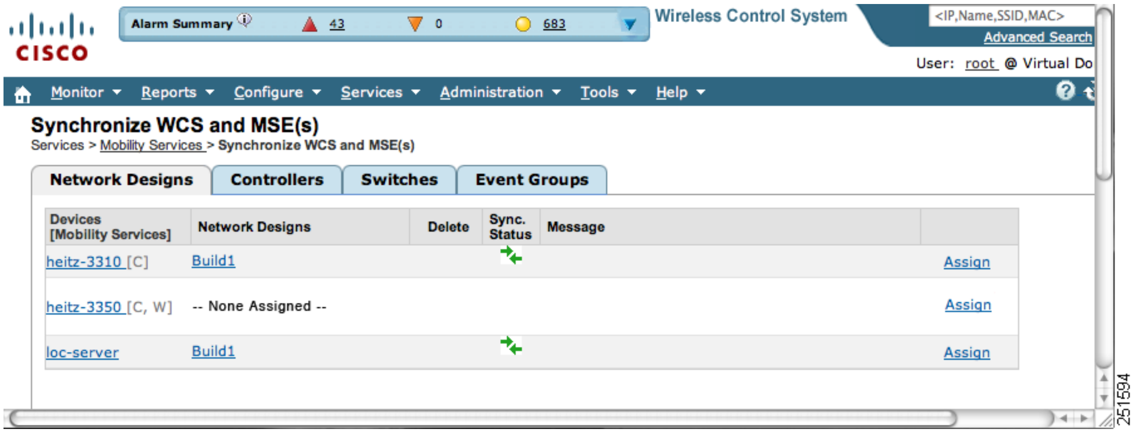
Note The Devices column appears on all four tabs and lists the name of the mobility services engine and the active services on that device. Services are noted in parenthesis next to the device name. Services supported are Context-Aware Software (C), and Wireless Intrusion Prevention Service (W).

Step 2 Select the appropriate tab (network designs, controllers, switches, or event groups).

a. To assign a network design to a mobility services engine, click the **Network Designs** tab (see Figure 3-1).

Note A network design might comprise a large campus with several buildings, each monitored by a different mobility services engine. Therefore, you might need to assign a single network design to multiple mobility services engines.

Figure 3-1 Services > Synchronize Services > Network Designs Window



Synchronize WCS and MSE(s)

Services > Mobility Services > Synchronize WCS and MSE(s)

Devices [Mobility Services]	Network Designs	Delete	Sync. Status	Message	
heitz-3310 [C]	Build1		⇄		Assign
heitz-3350 [C, W]	-- None Assigned --				Assign
loc-server	Build1		⇄		Assign

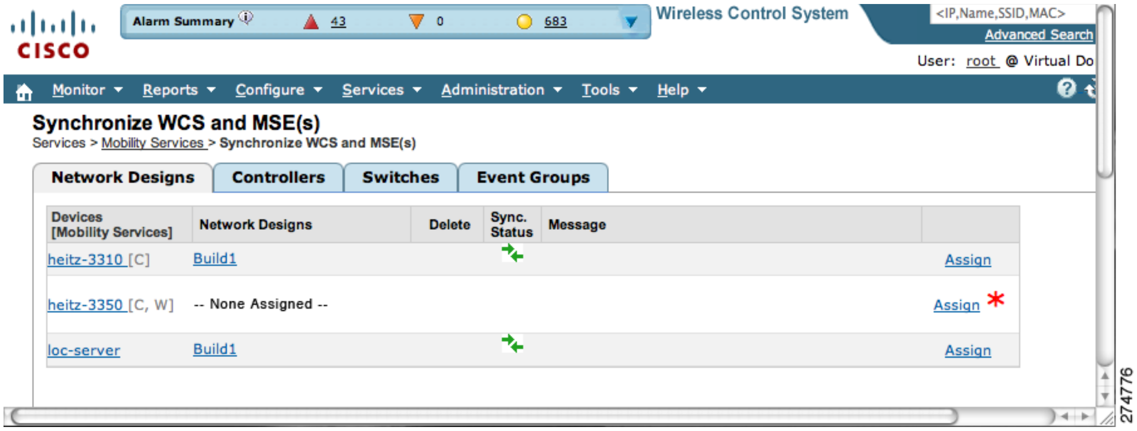
1. Click the **Assign** link for the appropriate network design.

2. In the Network Designs window that appears, check the check box of each network design that you want to apply to the mobility services engine. Click **OK** when the selection is complete.

   A red asterisk (*) appears next to the Assign link (see Figure 3-1).

   To undo assignments, click **Reset**. To go back to the Synchronize WCS and MSE(s) window without making any changes, click **Cancel**.

Figure 3-2 Services > Synchronize Services > Network Designs Window



Synchronize WCS and MSE(s)

Services > Mobility Services > Synchronize WCS and MSE(s)

Devices [Mobility Services]	Network Designs	Delete	Sync. Status	Message	
heitz-3310 [C]	Build1		⇄		Assign
heitz-3350 [C, W]	-- None Assigned --				Assign *
loc-server	Build1		⇄		Assign

3. Click **Synchronize** to update the mobility services database.

   When items are synchronized, a green two-arrow icon appears in the Sync. Status column for each synchronized entry.

b. To associate a mobility services engine with a controller, click the **Controllers** tab.

1. In the Controllers window that appears click the **Assign** link for that mobility services engine.

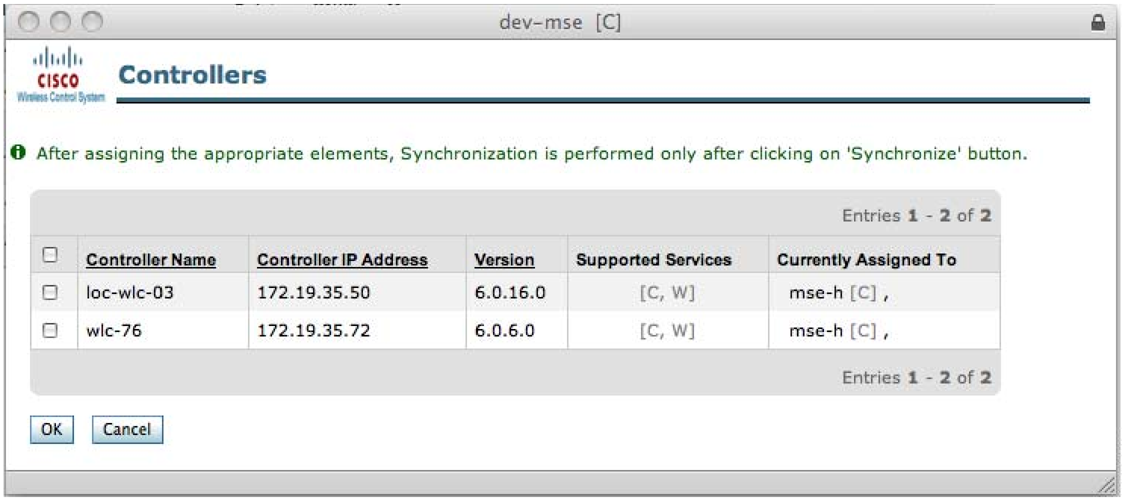
2. In the window that appears (see Figure 3-3), check the check box next to the appropriate controller. Click **OK**.

   The window in Figure 3-4 appears. A red asterisk (*) appears next to the Assign link

Note The selected controller must support the service that is configured on the mobility services engine (as noted in the supported services column). If it does not, a warning message appears when you click **OK**.

Note Controller names must be unique for synchronizing with a mobility services engine. If you have two controllers with the same name, only one controller synchronizes.

Figure 3-3 Controller Selection Window



Controllers

After assigning the appropriate elements, Synchronization is performed only after clicking on 'Synchronize' button.

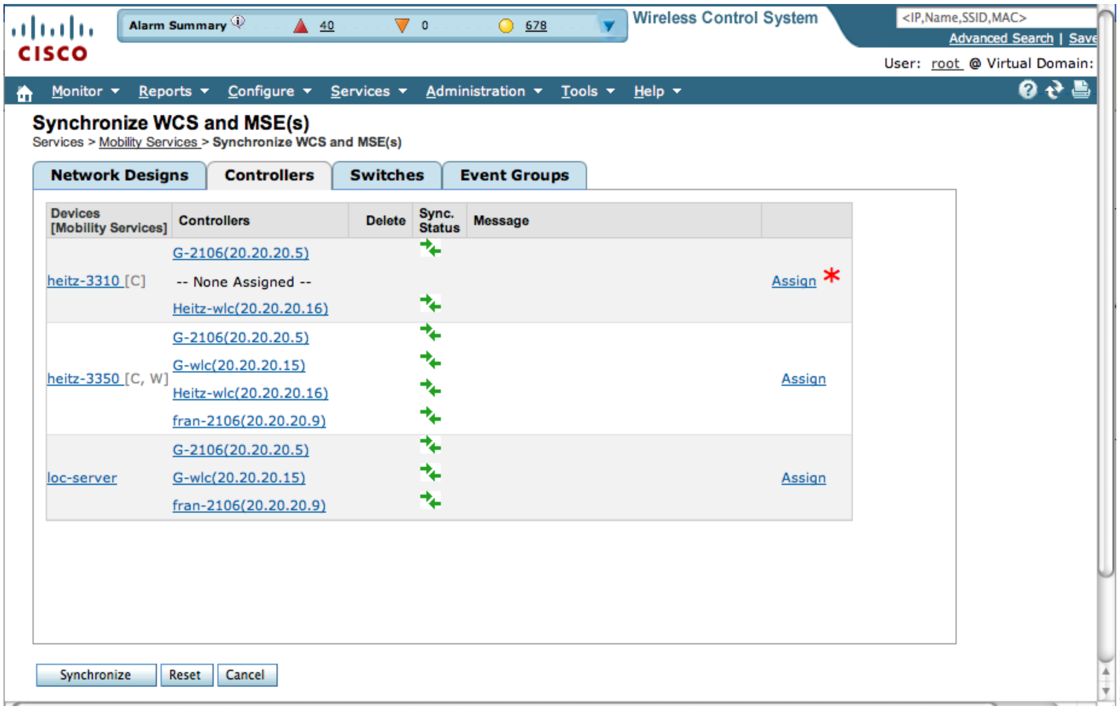
Entries 1 - 2 of 2

□	Controller Name	Controller IP Address	Version	Supported Services	Currently Assigned To
□	loc-wlc-03	172.19.35.50	6.0.16.0	[C, W]	mse-h [C] ,
□	wlc-76	172.19.35.72	6.0.6.0	[C, W]	mse-h [C] ,

Entries 1 - 2 of 2

276066

Figure 3-4 Services > Synchronize Services > Controllers Window



Synchronize WCS and MSE(s)

Services > Mobility Services > Synchronize WCS and MSE(s)

Devices [Mobility Services]	Controllers	Delete	Sync. Status	Message	

heitz-3310 [C]	G-2106(20.20.20.5)
	-- None Assigned --
	Heitz-wlc(20.20.20.16)
			✓
			
			✓
					Assign *

heitz-3350 [C, W]	G-2106(20.20.20.5)
	G-wlc(20.20.20.15)
	Heitz-wlc(20.20.20.16)
	fran-2106(20.20.20.9)
			✓
			✓
			✓
			✓
					Assign

loc-server	G-2106(20.20.20.5)
	G-wlc(20.20.20.15)
	fran-2106(20.20.20.9)
			✓
			✓
			✓
					Assign

274777

3. Click **Synchronize** to update the mobility services database.

   To undo assignments prior to synchronization, click **Reset**. To go back to the Synchronize WCS and MSE(s) window without making any changes, click **Cancel**.

   When items are synchronized, a green two-arrow icon appears in the Sync. Status column for each synchronized entry.

c. To assign a Catalyst switch to a mobility services engine, click the **Switches** tab (see Figure 3-5).

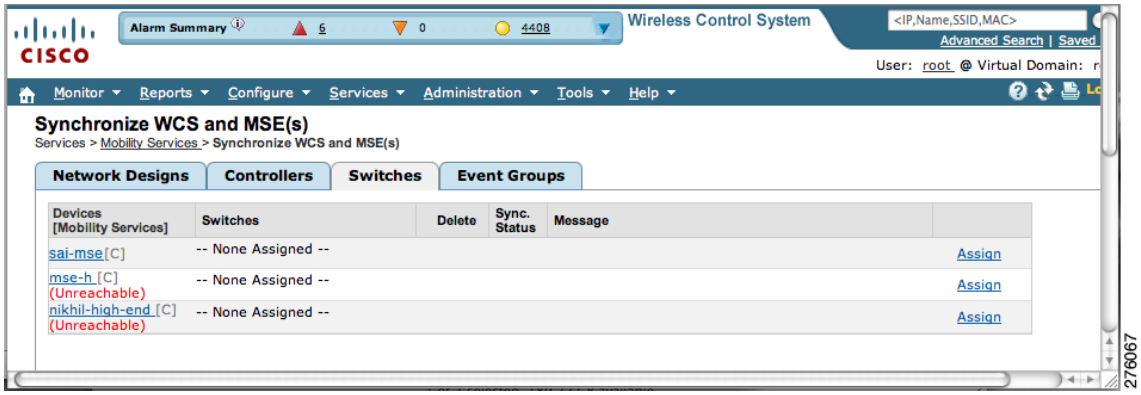
After adding a Catalyst switch to Cisco WCS, you need to assign it to a mobility services engine and then synchronize the two systems. Once they are synchronized, an NMSP connection between the switch and the mobility services engine is established.

All information (such as IP address, MAC, and civic address) on the wired switches and the wired clients connected to them downloads to the mobility services engine.

Note A switch can only be synchronized with one mobility services engine. However, a mobility services engine can have many switches attached to it.

1. To assign a Catalyst switch to a mobility services engine, click its corresponding **Assign** link.

Figure 3-5 Services > Synchronize Services > Switches Window

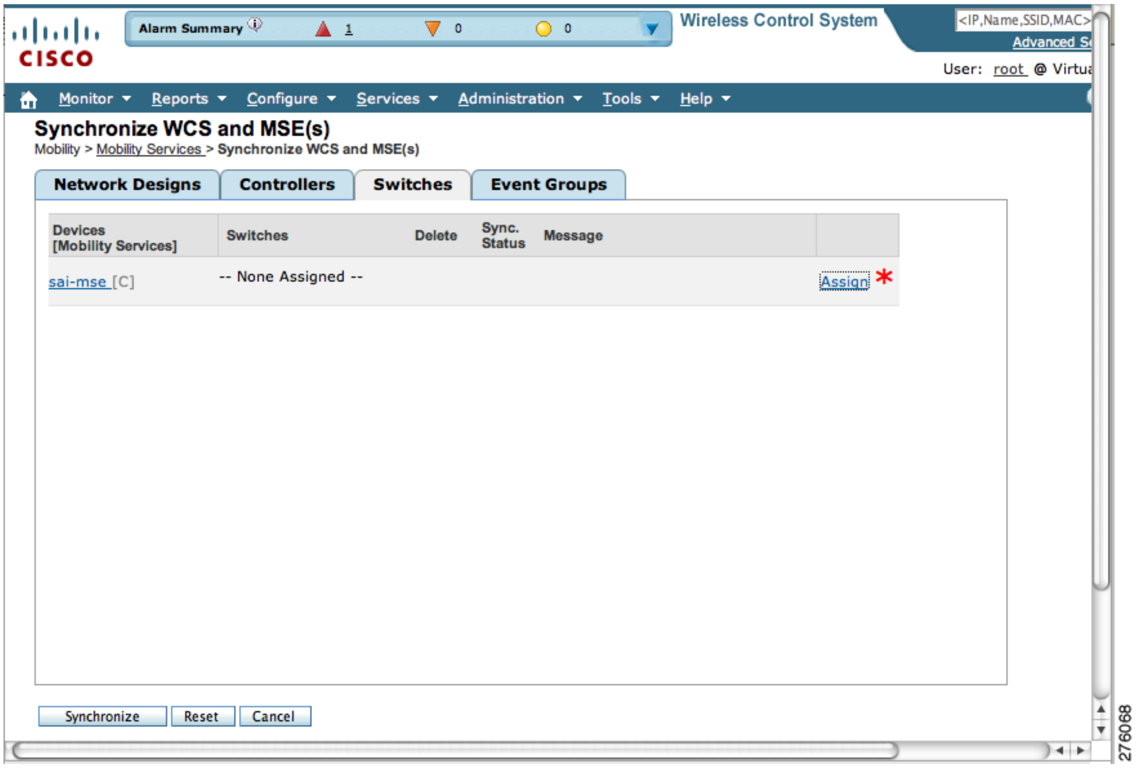


Devices [Mobility Services]	Switches	Delete	Sync. Status	Message	
sai-mse[C]	-- None Assigned --				Assign
mse-h [C] (Unreachable)	-- None Assigned --				Assign
nikhil-high-end [C] (Unreachable)	-- None Assigned --				Assign

2. In the Switch panel that appears, check the check box next to each wired switch to which you want the mobility services engine associated. Click **OK**.

A red asterisk (*) appears next to the Assign link (see Figure 3-6).

Figure 3-6 Services > Synchronize Services > Switches Window



Synchronize WCS and MSE(s)

Mobility > Mobility Services > Synchronize WCS and MSE(s)

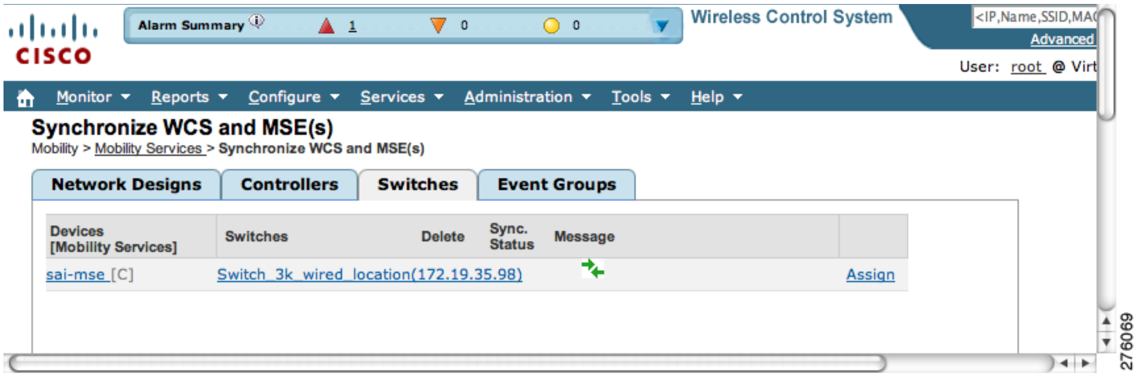
Devices [Mobility Services]	Switches	Delete	Sync. Status	Message	
sai-mse [C]	-- None Assigned --				Assign *

3. Click **Synchronize** to update the mobility services database.

   To undo assignments prior to synchronization, click **Reset**. To go back to the Synchronize WCS and MSE(s) window without making any changes, click **Cancel**.

   When items are synchronized, a green two-arrow icon appears in the Sync. Status column for each synchronized entry (see Figure 3-7).

Figure 3-7 Synchronize WCS and MSE Confirmation Window



Synchronize WCS and MSE(s)

Mobility > Mobility Services > Synchronize WCS and MSE(s)

Devices [Mobility Services]	Switches	Delete	Sync. Status	Message	
sai-mse [C]	Switch_3k_wired_location(172.19.35.98)		⇄		Assign

d. To assign an Event Group to a mobility services engine, click the **Event Groups** tab.

1. In the Event Groups panel that appears, check the check box for each event group that you want to assign to the mobility services engine. Click **OK**.

   A red asterisk (*) appears next to the Assign link. To undo assignments, click **Reset**. To go back to the Synchronize WCS and Server(s) window without making any changes, click **Cancel**.

2. Click **Synchronize** to update the mobility services database.

   To undo assignments prior to synchronization, click **Reset**. To go back to the Synchronize WCS and MSE(s) window without making any changes, click **Cancel**.

   When items are synchronized, a green two-arrow icon appears in the Sync. Status column for each synchronized entry.

Note To unassign a network design, controller, switch, or event group from a mobility services engine, click the **Assign** link next to the system. In the panel that appears, uncheck the check box for the corresponding network design, controller, switch, or event group. Click **OK.** Then, click **Synchronize**. The name of the removed network design, controller or event group is replaced with *None Assigned*.

Configuring Automatic Database Synchronization and Out of Sync Alerts

Manual synchronization of Cisco WCS and mobility services engine databases is immediate. However, future deployment changes (such as changes to maps and access point positions) can yield incorrect information until resynchronization.

To prevent out-of-sync conditions, use Cisco WCS to enable automatic synchronization. This policy ensures that synchronization between Cisco WCS and mobility services engine databases is triggered periodically and any related alarms are cleared.

To configure automatic synchronization, follow these steps:

Step 1 In Cisco WCS, choose **Administration > Background Tasks**.

Step 2 Check the **Mobility Service Synchronization** check box. Select **Enable Task** from the Select a command drop-down menu if not already enabled. Click **Go**.

Step 3 Click the **Mobility Service Synchronization** link. The Task > Mobility Service Synchronization window appears.

Step 4 To set the mobility services engine to send out-of-sync alerts, check the Out of Sync Alerts **Enabled** check box. By default, out-of-sync alarms are enabled.

Note Uncheck the Out of Sync Alerts **Enabled** check box to disable forwarding of out-of-sync alarms.

Note For a summary of out of sync alerts that are sent, refer to the "Out-of-Sync Alarms" section on page 3-9.

Step 5 To enable automatic synchronization, check the Auto Synchronization **Enabled** check box.

Note Automatic synchronization does not apply to network designs, controllers, switches, or event groups that have not yet been assigned to a mobility services engine. However, out-of-sync alarms will still be generated for these unassigned elements. For automatic synchronization to apply to network designs, controllers, switches, or event groups, you need to manually assign them to a mobility services engine.

Step 6 Enter the time interval in hours that the automatic synchronization is to be performed.

By default, auto-sync is disabled.

Step 7 Click **Submit**. You are returned to the **Administration > Background Tasks** screen and the Mobility Service Synchronization task displays an enabled state.

Out-of-Sync Alarms

Out-of-sync alarms are of minor severity (yellow), and are raised in response to the following conditions:

- Elements are modified in Cisco WCS (the auto-sync policy pushes these elements)
- Elements are modified in the mobility services engine (the auto-sync policy pulls these elements)
- Elements other than controllers exist in the mobility services engine database but not in Cisco WCS (the auto-sync policy pulls these elements)
- Elements are not assigned to any mobility services engine (the auto-sync policy does not apply)

Out-of-sync alarms are cleared when the following occurs:

- Mobility services engine is deleted

Note When you delete a mobility services engine, the out-of-sync alarms for that system are also deleted. In addition, if you delete the last available mobility services engine, the alarms for the following event: *elements not assigned to any server* will also be deleted.

- Elements are synchronized manually or automatically
- User manually clears the alarms (although the alarms may reappear in the future when the scheduled task is next executed)

Viewing Synchronization Information

This section describes how to view synchronization status and history.

Viewing Mobility Services Engine Synchronization Status

You can use the Synchronize Servers command in Cisco WCS 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 In Cisco WCS, choose **Services > Synchronize Services**.

Step 2 Select either the **Network Designs**, **Controllers**, **Switches,** or **Event Groups** tab.

In the panel that appears, check the Sync. Status column for the synchronization status. A green two-arrow icon indicates that the mobility services engine is synchronized with the specified network design, controller, wired Catalyst switch, or event group. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a given mobility services engine.

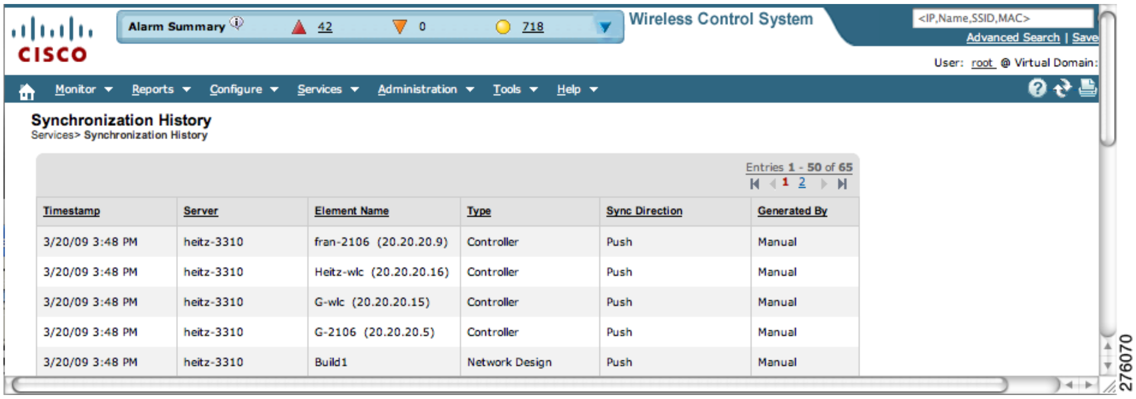
Viewing Synchronization History

You can 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, follow these steps:

Step 1 In Cisco WCS, choose **Services > Synchronization History**. The Synchronization History window appears (see Figure 3-8).

Figure 3-8 Services > Synchronization History



Synchronization History
Services> Synchronization History

Entries 1 - 50 of 65
1 2

Timestamp	Server	Element Name	Type	Sync Direction	Generated By
3/20/09 3:48 PM	heitz-3310	fran-2106 (20.20.20.9)	Controller	Push	Manual
3/20/09 3:48 PM	heitz-3310	Heitz-wlc (20.20.20.16)	Controller	Push	Manual
3/20/09 3:48 PM	heitz-3310	G-wlc (20.20.20.15)	Controller	Push	Manual
3/20/09 3:48 PM	heitz-3310	G-2106 (20.20.20.5)	Controller	Push	Manual
3/20/09 3:48 PM	heitz-3310	Build1	Network Design	Push	Manual

Step 2 Click the column headers to sort the entries.

In the Synchronization History window, the Sync Direction column indicates whether information is pushed into the mobility services engine or pulled by the mobility services engine. The Generated By column indicates whether the synchronization was manual or automatic.

CHAPTER 4

Configuring and Viewing System Properties

This chapter describes how to configure and view system properties on the mobility services engine.

This chapter contains the following sections:

Editing General Properties and Viewing Performance

General Properties—You can use Cisco WCS to edit the general properties of a mobility services engine such as contact name, username, password, services enabled on the system, and the number of remaining units on each active license. Refer to the "Editing General Properties" section on page 4-2.

Note You would use the general properties to modify the username and password that you defined during initial setup of the mobility services engine.

Performance—You can use Cisco WCS to view CPU and memory use for a given mobility services engine. Refer to the "Viewing Performance Information" section on page 4-5.

Editing General Properties

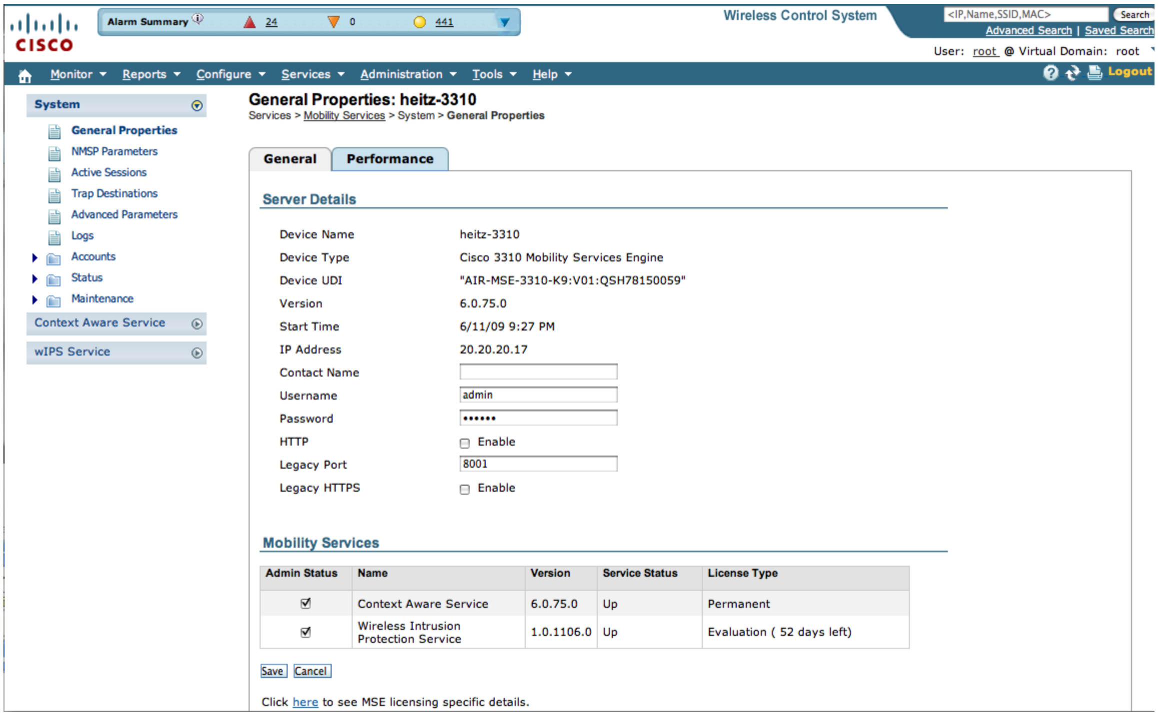
To edit the general properties of a mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services** to display the Mobility Services window.

Step 2 Click the name of the mobility services engine you want to edit. A two-tabbed panel labeled with General and Performance appears.

Note If the General Properties window does not display by default, select **General Properties** from the **Systems** menu left panel.

Figure 4-1 General Properties



General Properties: heitz-3310

Services > Mobility Services > System > General Properties

Server Details

Device Name	heitz-3310
Device Type	Cisco 3310 Mobility Services Engine
Device UDI	"AIR-MSE-3310-K9:V01:QSH78150059"
Version	6.0.75.0
Start Time	6/11/09 9:27 PM
IP Address	20.20.20.17
Contact Name	
Username	admin
Password	••••••
HTTP	□ Enable
Legacy Port	8001
Legacy HTTPS	□ Enable

Mobility Services

Admin Status	Name	Version	Service Status	License Type
☑	Context Aware Service	6.0.75.0	Up	Permanent
☑	Wireless Intrusion Protection Service	1.0.1106.0	Up	Evaluation (52 days left)

Click here to see MSE licensing specific details.

Step 3 Modify the parameters as appropriate in the **General** panel. Table 4-1 describes each parameter.

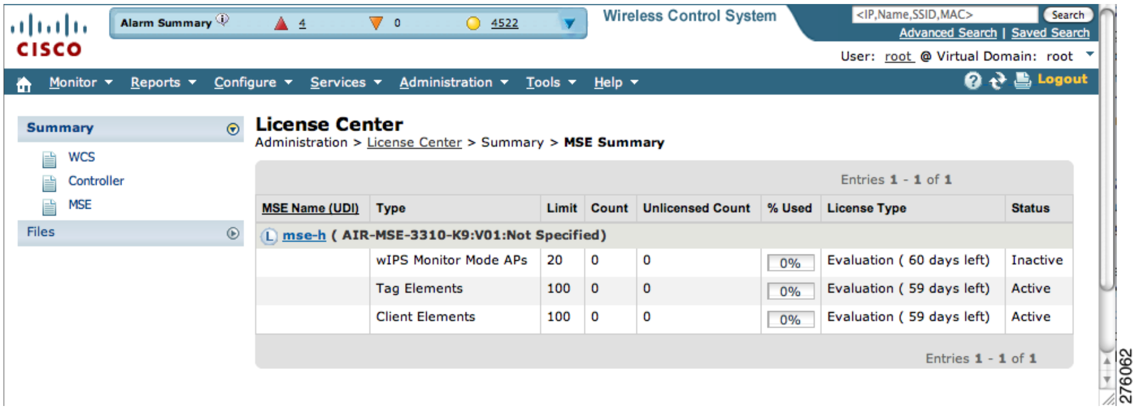
Table 4-1 General Properties

Parameter	Configuration Options
Contact Name	Enter a contact name for the mobility services engine.
User Name	Enter the login user name for the Cisco WCS server that manages the mobility services engine.
Password	Enter the login password for the Cisco WCS server that manages the mobility services engine.
Legacy Port	Enter the mobility services port number that supports HTTPS communication. The Legacy HTTPS option must also be enabled to provide connection to Cisco WCS.
HTTP	Check the **Enable** check box to enable HTTP. By default, HTTPS is enabled. **Note** HTTP is primarily enabled to allow third-party applications to communicate with the mobility services engine. **Note** Cisco WCS always communicates through HTTPS.
Legacy HTTPS	This parameter does not apply to mobility services engines. It applies only to location appliances.
Mobility Services	To enable a service (CAS, wIPS) on a mobility services engine, check the **Admin Status** check box next to the service you want to enable. **Note** Once selected, the service displays as Up (active). All inactive services are noted as Down (inactive) on the selected (current) system and on the network. **Note** CAS and wIPS can operate on a mobility services engine at the same time. **Note** All mobility services engines are shipped with an evaluation license of CAS and wIPS. Evaluation copies are good for a period of 60 days (480 hours) and have preset device limits for each service. Licenses are usage-based (time is decremented by the number of days you use it rather than by calendar days passed). Click the **here** link (bottom) to see the time remaining on service licenses (evaluation or purchased) and the number of devices that can be assigned for the current system (see Figure 4-1). On the license summary page (see Figure 4-2), click **MSE** (left) to see details on licenses for all mobility services engines on the network (see Figure 4-3). **Note** For more information on purchasing and installing licenses, refer to: http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

Note The following tcp ports are in use on a mobility services engine (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 could vary from 1 to 10), and tcp 8001: Legacy port. Used for location APIs. Change in Cisco WCS.

Note The following udp ports are in use on a mobility services engine (MSE) in release 6.0: udp 123: NTPD port (open after NTP configuration), udp 162: AeroScout SNMP, udp/tcp 4000X: AeroScout proxy (X could 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.

Figure 4-2 License Summary for Selected Mobility Services Engine



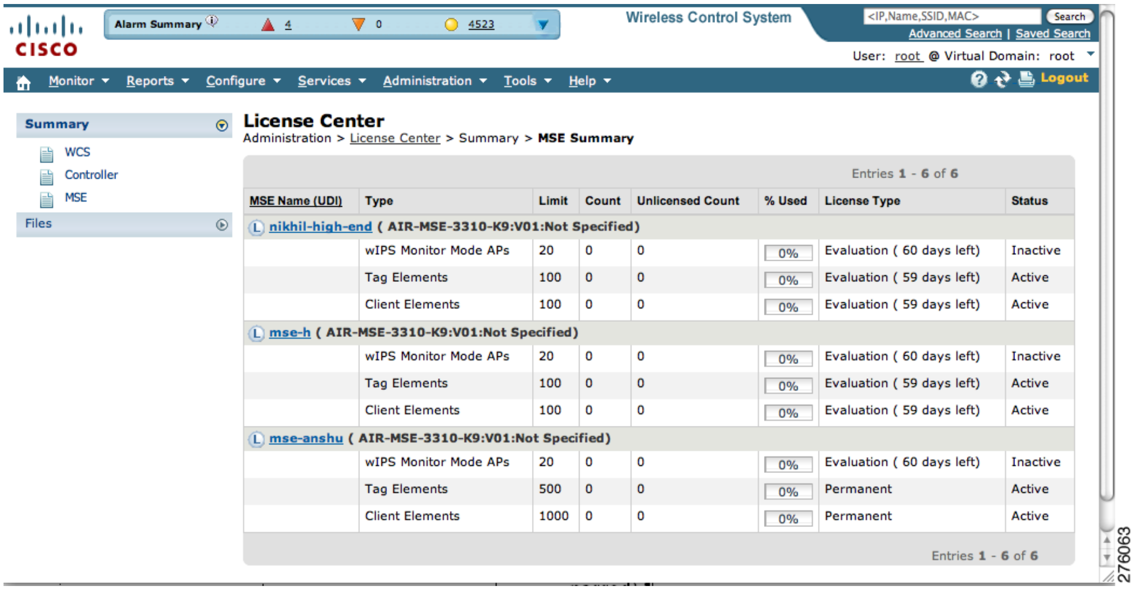
License Center
Administration > License Center > Summary > **MSE Summary**

Entries **1** - **1** of **1**

MSE Name (UDI)	Type	Limit	Count	Unlicensed Count	% Used	License Type	Status
mse-h (AIR-MSE-3310-K9:V01:Not Specified)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (60 days left)	Inactive
	Tag Elements	100	0	0	0%	Evaluation (59 days left)	Active
	Client Elements	100	0	0	0%	Evaluation (59 days left)	Active

Entries **1** - **1** of **1**

Figure 4-3 License Summary for All Mobility Services Engines



License Center
Administration > License Center > Summary > **MSE Summary**

Entries **1** - **6** of **6**

MSE Name (UDI)	Type	Limit	Count	Unlicensed Count	% Used	License Type	Status
nikhil-high-end (AIR-MSE-3310-K9:V01:Not Specified)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (60 days left)	Inactive
	Tag Elements	100	0	0	0%	Evaluation (59 days left)	Active
	Client Elements	100	0	0	0%	Evaluation (59 days left)	Active
mse-h (AIR-MSE-3310-K9:V01:Not Specified)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (60 days left)	Inactive
	Tag Elements	100	0	0	0%	Evaluation (59 days left)	Active
	Client Elements	100	0	0	0%	Evaluation (59 days left)	Active
mse-anshu (AIR-MSE-3310-K9:V01:Not Specified)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (60 days left)	Inactive
	Tag Elements	500	0	0	0%	Permanent	Active
	Client Elements	1000	0	0	0%	Permanent	Active

Entries **1** - **6** of **6**

Step 4 Click **Save** to update the Cisco WCS and mobility services engine databases.

Viewing Performance Information

To view performance details, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services** to display the Mobility Services window.

Step 2 Click the name of the mobility services engine you want to view. A two-tabbed panel appears with the following headings: General and Performance.

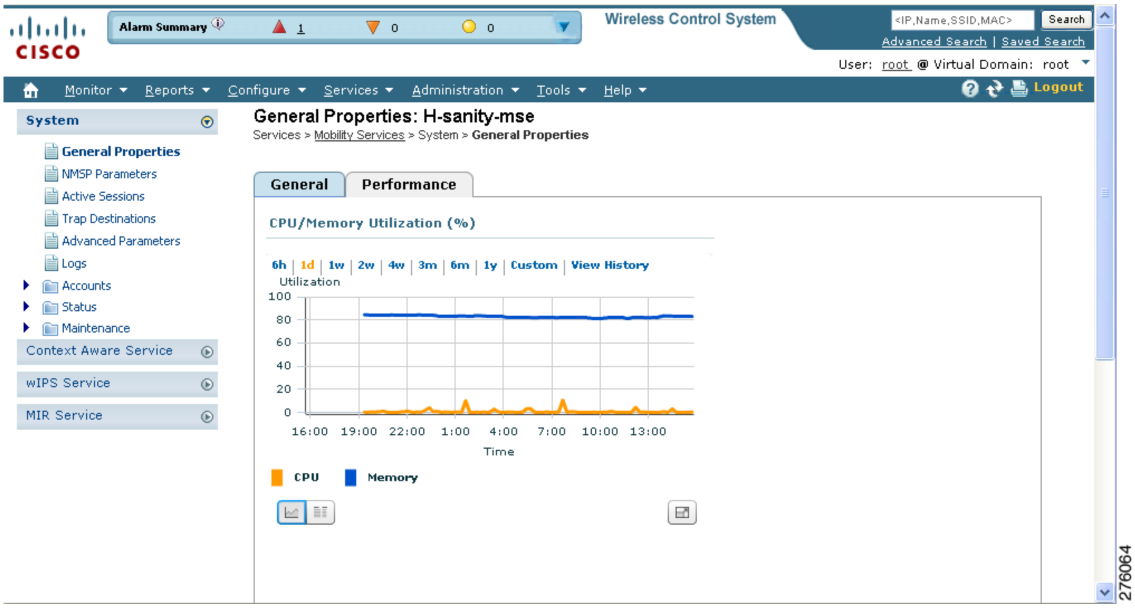
Step 3 Click **Performance** tab (see Figure 4-4).

Click a time period (such as *1w*) on the y-axis to see performance numbers for periods greater than one day.

To view a textual summary of performance, click the second icon under CPU.

To enlarge the screen, click the icon at the lower right.

Figure 4-4 CPU and Memory Performance



Modifying NMSP Parameters

Network Mobility Services Protocol (NMSP) is the protocol that manages communication between the mobility services engine and the controller or selected Catalyst 3000 and 4000 series switches. Transport of telemetry, emergency, and chokepoint information between the mobility services engine and the controller and Catalyst switch is managed by this protocol.

Note No change in the default parameter values is recommended unless the network is experiencing slow response or excessive latency.

- Telemetry, emergency, and chokepoint information is only seen on controllers and Cisco WCS installed with release 4.1 software or later.
- The TCP port (16113) that the controller or Catalyst switch and the mobility services engine communicate over MUST be open (not blocked) on any firewall that exists between the controller or Catalyst switch and mobility services engine for NMSP to function.

To configure NMSP parameters, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services.**

Step 2 Click the name of the mobility services engine whose properties you want to edit.

Step 3 Choose **System > NMSP Parameters** (left panel). The configuration options appear.

Step 4 Modify the NMSP parameters as appropriate. Table 4-2 describes each parameter.

Table 4-2 NMSP Parameters

Parameter	Description
Echo Interval	How frequently an echo request is sent from a mobility services engine 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 services engine 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	How long the mobility services engine waits before considering the pending request as timed out. The default value is 1 second. Minimum value is one (1). There is no maximum value.
Retransmit Interval	Interval of time that the mobility services engine 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	The maximum number of retransmits that are sent 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 Cisco WCS and mobility services engine databases.

Viewing Active Sessions on a System

You can view active user sessions on the mobility services engine.

For every session, Cisco WCS displays the following information:

- Session identifier
- IP address from which the mobility services engine is accessed
- Surname of the connected user
- Date and time when the session started
- Date and time when the mobility services engine was last accessed
- How long the session was idle since it was last accessed

To view active user sessions, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine on which you want to view active sessions.

Step 3 Choose **System > Active Sessions**.

Adding and Deleting Trap Destinations

You can specify which Cisco WCS 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.

When a user adds a mobility services engine using Cisco WCS, that WCS platform automatically establishes itself as the default trap destination. If a redundant Cisco WCS configuration exists, the backup WCS is not listed as the default trap destination unless the primary WCS fails and the back system takes over. Only an active Cisco WCS is listed as a trap destination.

Adding Trap Destinations

To add a trap destination, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine for which you want to define a new SNMP trap destination server.

Step 3 Choose **System > Trap Destinations**.

Step 4 Select **Add Trap Destination** from the Select a command drop-down menu. Click **Go**.

Step 5 Enter IP address of destination SNMP server.

Step 6 Port number default of *162* is auto-populated. You can modify this as needed.

Step 7 Community default value of *public* is auto-populated. You can modify this as needed.

Step 8 Destination default value of *other* auto-populates.

Note All trap destinations are identified as *other* except for the automatically created *default* trap destination.

Step 9 Click **Save**.

You are returned to the trap destinations summary window and the newly-defined trap is listed.

Deleting Trap Destinations

To delete a trap destination, follow these steps;

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine for which you want to delete a SNMP trap destination server.

Step 3 Choose **System** > **Trap Destinations**.

Step 4 Check the check box next to the trap destination entry that you want to delete.

Step 5 Select **Delete Trap Destination** from the Select a command drop-down menu. Click **Go**.

Step 6 In the message box that appears, click **OK** to confirm deletion.

Viewing and Configuring Advanced Parameters

In Cisco WCS, at the Advanced Parameters window (see Figure 4-5) you can both view general system level settings of the mobility services engine and configure monitoring parameters.

- Refer to the "Viewing Advanced Parameters Settings" section on page 4-8 to view current system-level advanced parameters.
- Refer to the "Initiating Advanced Commands" section on page 4-10 to modify the current system-level advanced parameters or initiate advanced commands such as system reboot, system shutdown, clear a configuration file, or defragment the system database.

Viewing Advanced Parameters Settings

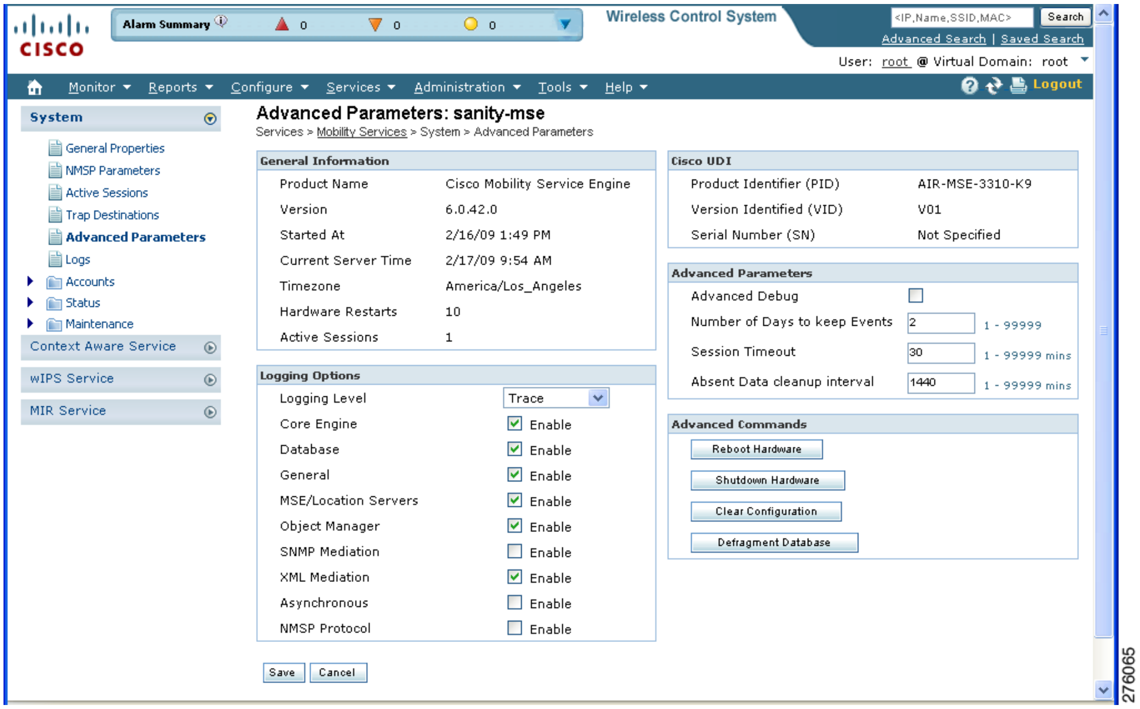
To view the advanced parameter settings of the mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services.**

Step 2 Click the name of a mobility services engine to view its status.

Step 3 Choose **System** > **Advanced Parameters** (left panel). The following window appears (see Figure 4-5).

Figure 4-5 Services > Mobility Services > System > Advanced Parameters



Advanced Parameters: sanity-mse

Services > Mobility Services > System > Advanced Parameters

General Information

Product Name	Cisco Mobility Service Engine
Version	6.0.42.0
Started At	2/16/09 1:49 PM
Current Server Time	2/17/09 9:54 AM
Timezone	America/Los_Angeles
Hardware Restarts	10
Active Sessions	1

Cisco UDI

Product Identifier (PID)	AIR-MSE-3310-K9
Version Identified (VID)	V01
Serial Number (SN)	Not Specified

Advanced Parameters

Advanced Debug	□	
Number of Days to keep Events	2	1 - 99999
Session Timeout	30	1 - 99999 mins
Absent Data cleanup interval	1440	1 - 99999 mins

Logging Options

Logging Level	Trace
Core Engine	☑ Enable
Database	☑ Enable
General	☑ Enable
MSE/Location Servers	☑ Enable
Object Manager	☑ Enable
SNMP Mediation	□ Enable
XML Mediation	☑ Enable
Asynchronous	□ Enable
NMSP Protocol	□ Enable

Advanced Commands

Initiating Advanced Parameters

On the Advanced Parameters window, you can use Cisco WCS:

- To specify the logging level and types of messages to log.

  Refer to the "Configuring Logging Options" section on page 4-9.

- To set how long events are kept, how long before a session time-outs, and the interval between data clean ups.

  Refer to the "Configuring Advanced Parameters" section on page 4-10.

- To enable or disable advanced debug level messages in the logs.

  Refer to the "Configuring Advanced Parameters" section on page 4-10.

Configuring Logging Options

You can use Cisco WCS to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to configure.

Step 3 Choose **System > Advanced Parameters**. The advanced parameters for the selected mobility services engine appears.

Step 4 Scroll down to the Logging Options section and choose the appropriate option from the Logging Level drop-down menu.

There are four logging options: **Off**, **Error**, **Information**, and **Trace**.

Caution Use **Error** and **Trace** only when directed to do so by Cisco Technical Assistance Center (TAC) personnel.

Step 5 Check the **Enabled** check box next to each item listed in that section to begin logging of its events.

Step 6 Click **Save**.

Configuring Advanced Parameters

To configure advanced parameters, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to configure.

Step 3 Choose **System > Advanced Parameters**. The advanced parameters for the selected mobility services engine appears.

Step 4 Scroll down to the Advanced Parameters and make the appropriate changes. Table 4-3 describes the parameters.

Table 4-3 Advanced Parameters

Parameter	Configuration Options
Advanced debug	Check the check box to enable advanced debug. This enables reporting of advanced debug level messages to the log files.
Number of days to keep events	Enter the number of days that events are kept in the event table. Default value is 2.
Session time-out (minutes)	Enter the number of minutes a Cisco WCS or client session can remain inactive before it times out. Default value is 30.
Absent data cleanup interval (minutes)	Enter the number of minutes that data for *absent* mobile stations is kept. An *absent* mobile station is one that was discovered but does not appear in the network. Default value is 1440.

Initiating Advanced Commands

You can initiate a system reboot or shutdown, clear the system configuration or defragment a database by clicking the appropriate button on the Advanced Parameters page.

Rebooting or Shutting Down a System

To reboot or shutdown a mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services.**

Step 2 Click the name of a mobility services engine you want to reboot or shutdown

Step 3 Choose **System > Advanced Parameters** (left panel).

Step 4 In the Advanced Commands section of the window (right), click the appropriate button (**Reboot Hardware** or **Shutdown Hardware**).

Click **OK** in the confirmation pop-up window to initiate either the reboot or shutdown process. Click **Cancel** to stop the process.

Clearing the System Database

To clear the database of a mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Mobility > Mobility Services.**

Step 2 Click the name of a mobility services engine whose database you want to clear.

Step 3 Choose **System > Advanced Parameters** (left panel).

Step 4 In the Advanced Commands section of the window (right), click the **Clear Configuration** button.

Note The Clear Configuration button is mislabeled. It clears the database not the configuration file.

Click **OK** in the confirmation pop-up window to initiate the process. Click **Cancel** to stop the process.

Defragment Database

To defragment the database of a mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services.**

Step 2 Click the name of a mobility services engine for which you want to clear its configuration file.

Step 3 Choose **System > Advanced Parameters** (left panel).

Step 4 In the Advanced Commands section of the window (right), click the **Defragment Database** button.

Click **OK** in the confirmation pop-up window to initiate the process. Click **Cancel** to stop the process.

CHAPTER 5

Managing Users and Groups

This chapter describes how to configure and manage users, groups, and host access on the mobility services engine.

This chapter contains the following sections:

- Managing Groups, page 5-2
- Managing Users, page 5-3

Managing Groups

This section describes how to add, delete, and edit user groups.

User groups allow you to define and different access privileges to users.

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 will not be able to configure mobility services engine settings.

Adding User Groups

To add a user group to a mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine to which you want to add a user group.

Step 3 Choose **System > Accounts > Groups** (left).

Step 4 Select **Add Group** from the Select a command drop-down menu and click **Go**.

Step 5 Enter the name of the group in the Group Name field.

Step 6 Select a permission level (read, write, or full) from the Permission drop-down menu.

Note Full Access is required for Cisco WCS to access mobility services engines.

Step 7 Click **Save**.

Deleting User Groups

To delete user groups from a mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine from which you want to delete a user group.

Step 3 Choose **System > Accounts > Groups** (left).

Step 4 Check the check boxes of the groups that you want to delete.

Step 5 Select **Delete Group** from the Select a command drop-down menu and click **Go**.

Step 6 Click **OK**.

Changing User Group Permissions

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 will not be able to configure mobility services engine settings.

To change user group permissions, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine you want to edit.

Step 3 Choose **System > Accounts > Groups** (left).

Step 4 Click the name of the group you want to edit.

Step 5 Select a permission level (read, write, or full) from the Permission drop-down menu.

Step 6 Click **Save**.

Managing Users

This section describes how to add, delete, and edit users to a mobility services engine. It also describes how to view active user sessions.

Adding Users

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 will not be able to configure mobility services engine settings.

To add a users to a mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine to which you want to add users.

Step 3 Choose **System > Accounts > Users** (left).

Step 4 Select **Add User** from the Select a command drop-down menu and click **Go**.

Step 5 Enter the username in the Username field.

Step 6 Enter a password in the Password field.

Step 7 Enter the name of the group to which the user belongs in the Group Name field.

Step 8 Select a permission level (read, write, or full) from the Permission drop-down menu.

Note Full Access is required for Cisco WCS to access mobility services engines.

Step 9 Click **Save**.

Deleting Users

To delete a user from a mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine from which you want to delete a user.

Step 3 Choose **System > Accounts > Users** (left).

Step 4 Check the check boxes of the users that you want to delete.

Step 5 Select **Delete User** from the Select a command drop-down menu and click **Go**.

Step 6 Click **OK**.

Changing User Properties

To change user properties, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine you want to edit.

Step 3 Choose **System > Accounts > Users** (left).

Step 4 Click the name of the group that you want to edit.

Step 5 Make the required changes to the Password, Group Name, and Permission fields.

Step 6 Click **Save**.

CHAPTER 6

Configuring wIPS and Profiles

This chapter describes how to configure wIPS profiles and those items that must be configured in conjunction to operate wIPS.

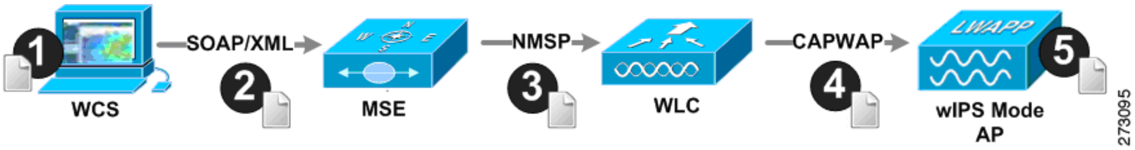
This chapter contains the following sections:

Overview of wIPS Configuration and Profile Management

Configuration of wIPS profiles follows a chained hierarchy starting with WCS which is used for profile viewing and modification. The actual profiles are stored within the wIPS service running on the mobility services engine (MSE).

From the wIPS service on the mobility services engine, profiles are propagated to specific controllers which in turn communicate this profile transparently to wIPS mode access points associated to that respective controller.

Figure 6-1 Configuration and Update of wIPS Profiles



When a configuration change to a wIPS profile is made at WCS and applied to a set of mobility services engines and controllers, the following occurs:

1. The configuration profile is modified on WCS and version information is updated.
2. An XML-based profile is pushed to the wIPS engine running on the mobility services engine. This update occurs over the SOAP/XML protocol.
3. The wIPS engine on the mobility services engine updates each controller associated with that profile by pushing out the configuration profile over NMSP.

Note A controller is associated to a single configuration profile. All wIPS mode access points connected to that controller share the same wIPS configuration.

4. The controller receives the updated wIPS profile, stores it into NVRAM (replacing any previous revision of the profile) and propagates the updated profile to its associated wIPS access points using CAPWAP control messages.
5. A wIPS mode access point receives the updated profile from the controller and applies the modifications to its wIPS software engine.

Note The mobility services engine can only be configured from one Cisco WCS.

Before you can configure wIPS profiles you must do the following:

1. Install a mobility services engine (if one is not already operating in the network). Refer to the *Cisco 3350 Mobility Services Engine Getting Started Guide* or *Cisco 3310 Mobility Services Engine Getting Started Guide* at:
   http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html
2. Add the mobility services engine to Cisco WCS (if not already added). Refer to Chapter 2, "Adding and Deleting Systems"
3. Configure access points to operate in wIPS monitor mode. Refer to "Configuring Access Points for wIPS Monitor Mode" section on page 6-3.
4. Configure wIPS profiles. Refer to "Configuring wIPS Profiles" section on page 6-4.

Configuring Access Points for wIPS Monitor Mode

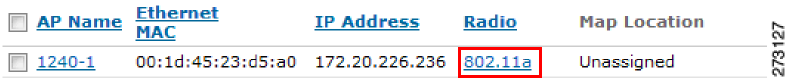
Note Only Cisco Aironet 1130, 1140, 1240, and 1250 Series Access Points support wIPS monitor mode.

To configure an access point to operate in wIPS monitor mode, follow these steps:

Step 1 In Cisco WCS, choose **Configure** > **Access Points**.

Step 2 Click on the 802.11a or 802.11b/g radio (see Figure 6-2).

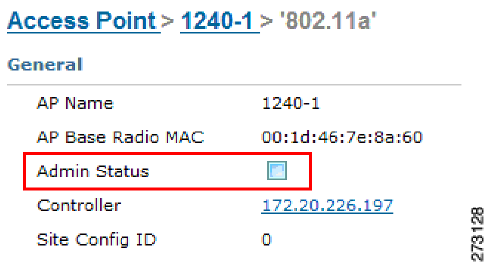
Figure 6-2 Configure > Access Points > Radio



□	AP Name	Ethernet MAC	IP Address	Radio	Map Location
□	1240-1	00:1d:45:23:d5:a0	172.20.226.236	802.11a	Unassigned

Step 3 On the access point window, uncheck **Admin Status** to disable the radio.

Figure 6-3 Access Points > Radio



Access Point > 1240-1 > '802.11a'

General

AP Name	1240-1
AP Base Radio MAC	00:1d:46:7e:8a:60
Admin Status	□
Controller	172.20.226.197
Site Config ID	0

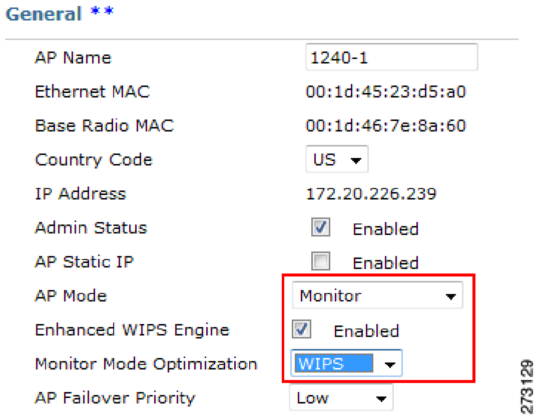
Step 4 Click **Save** (bottom).

Note Repeat these steps for each and every radio on an access point that is to be configured for wIPS monitor mode. For example, an Aironet 1130 requires this step to be performed on both its 802.11a and 802.11b/g radios.

Step 5 Once the radios are disabled, click **Configure > Access Points** and then click on the name of the access point whose radio you just disabled.

Step 6 At the access point configuration window, select **Monitor Mode** from the AP Mode drop-down menu. (see Figure 6-4).

Figure 6-4 Configure > Access Points > AP Name



General **

AP Name	1240-1
Ethernet MAC	00:1d:45:23:d5:a0
Base Radio MAC	00:1d:46:7e:8a:60
Country Code	US ▾
IP Address	172.20.226.239
Admin Status	☑ Enabled
AP Static IP	□ Enabled
AP Mode	Monitor ▾
Enhanced WIPS Engine	☑ Enabled
Monitor Mode Optimization	WIPS ▾
AP Failover Priority	Low ▾

Step 7 Check the **Enabled** check box for the Enhanced WIPS Engine.

Step 8 Select **WIPS** from the Monitor Mode Optimization drop-down menu.

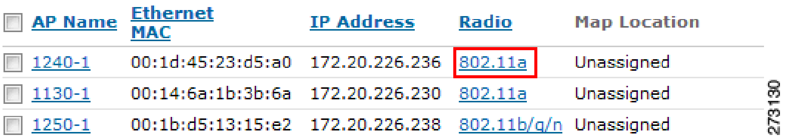
Step 9 Click **Save**.

Step 10 Click **OK** when prompted to reboot the access point.

Step 11 To reenable the access point radio, choose **Configure > Access Points**.

Step 12 Click on the appropriate access point radio (see Figure 6-5).

Figure 6-5 Configure > Access Points > Radio



□ AP Name	Ethernet MAC	IP Address	Radio	Map Location
□ 1240-1	00:1d:45:23:d5:a0	172.20.226.236	802.11a	Unassigned
□ 1130-1	00:14:6a:1b:3b:6a	172.20.226.230	802.11a	Unassigned
□ 1250-1	00:1b:d5:13:15:e2	172.20.226.238	802.11b/g/n	Unassigned

Step 13 At the radio configuration panel, check the Admin Status **Enabled** check box.

Step 14 Click **Save**.

Repeat this for each access point and each respective radio configured for wIPS monitor mode.

Configuring wIPS Profiles

By default, the mobility services engine and corresponding wIPS access points inherit the default wIPS profile from WCS. This profile comes pre-tuned with a majority of attack alarms enabled by default and will monitor attacks against access points within the same RF-Group as the wIPS access points. In this manner, the system comes pre-setup to monitor attacks against a deployment model that utilizes an integrated solution in which both the WLAN infrastructure and wIPS access points are intermixed on the same controller.

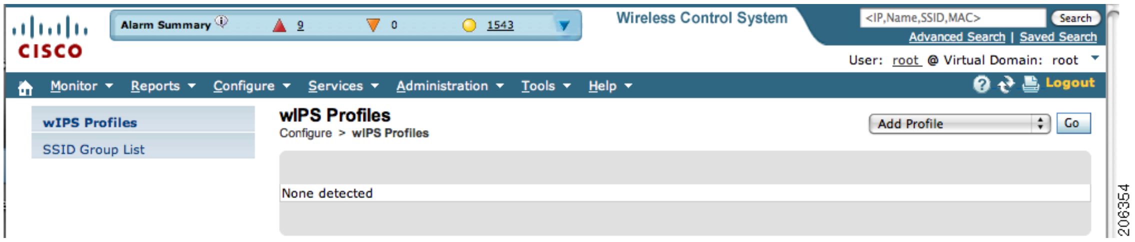
Note Some of the configuration steps that follow are marked as *Overlay-Only* and are only to be undertaken when deploying the Adaptive wIPS solution to monitor an existing WLAN Infrastructure such as an autonomous or completely separate controller-based WLAN.

To configure wIPS profiles, follow these steps:

Step 1 In Cisco WCS, choose **Configure > wIPS Profiles**.

Step 2 In the window that appears (Figure 6-6), select **wIPS Profiles** (left panel).

Figure 6-6 WIPS Profiles > Profile List



User: root @ Virtual Domain: root

wIPS Profiles
Configure > wIPS Profiles

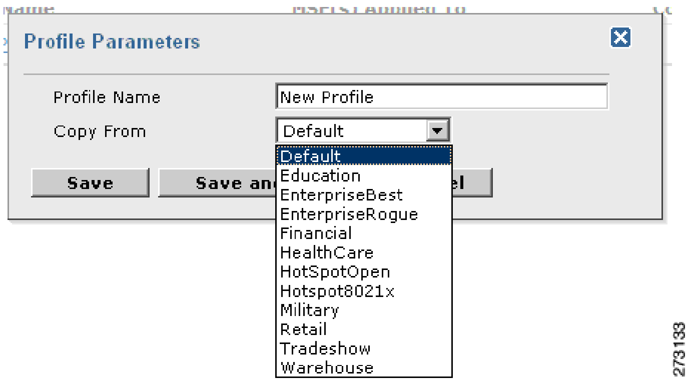
None detected

Step 3 Select **Add Profile** from the Select a command drop-down menu. Click **Go**.

Step 4 At the profile parameters panel, select a profile template from the Copy From drop-down menu (see Figure 6-7).

Note Cisco's Adaptive wIPS comes with a pre-defined set of profile templates from which customers can choose from or use as a basis for their own custom profiles. Each profile is tailored to either a specific business or application as are the specific alarms enabled on that profile.

Figure 6-7 Profile Parameters Configuration Panel



Profile Parameters

Profile Name: New Profile

Copy From: Default

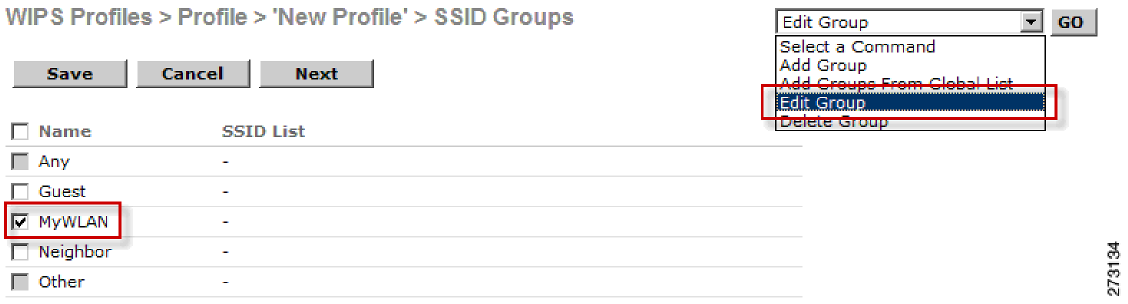
Step 5 After selecting a profile and entering a profile name, click **Save and Edit**.

Step 6 (Optional) Configure the SSIDs to Monitor (see Figure 6-8).

By default, the system monitors attacks launched against the local Wireless LAN Infrastructure (as defined by APs which have the same RF Group name). If the system should also be required to monitor attacks against another network, such as when deployed in an overlay deployment model, the SSID groups feature must be utilized.

Note If this step is not required, simply click **Next**.

Figure 6-8 SSID Groups Summary Panel


WIPS Profiles > Profile > 'New Profile' > SSID Groups
Save
Cancel
Next
Edit Group
GO
Select a Command
Add Group
Add Groups From Global List
Edit Group
Delete Group
273134

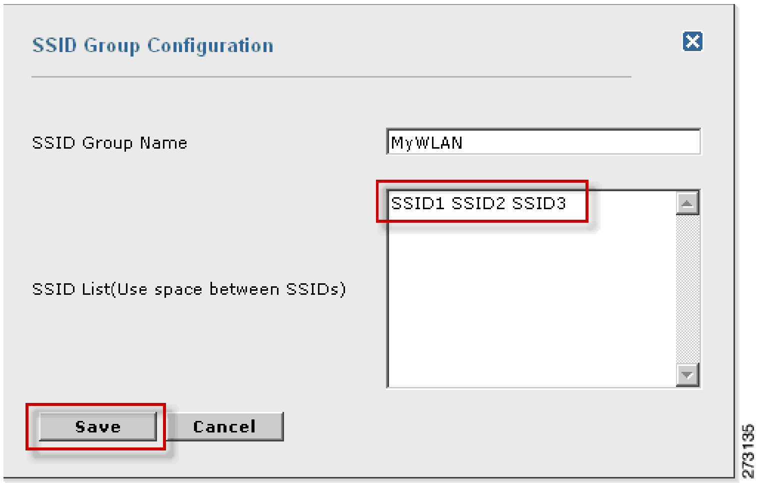
□ Name	SSID List
□ Any	-
□ Guest	-
☑ MyWLAN	-
□ Neighbor	-
□ Other	-

a. Check the box next to **MyWLAN** and select **Edit Group** from the drop down in the upper right hand corner then click **GO.**

b. Enter SSIDs to Monitor.

c. Enter the SSID name (separate multiple entries by a single space) and click **Save** (see Figure 6-9).

Figure 6-9 SSID Group Configuration Panel

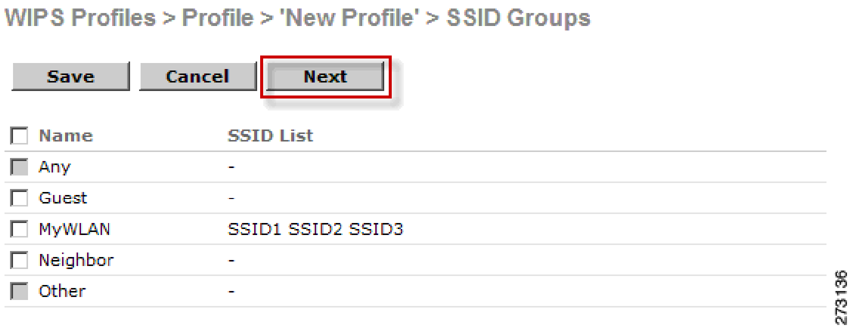


SSID Group Name: MyWLAN

SSID List(Use space between SSIDs): SSID1 SSID2 SSID3

The SSID Groups page appears confirming the SSID are added successfully (see Figure 6-10).

Figure 6-10 New Profile > SSID Groups Window

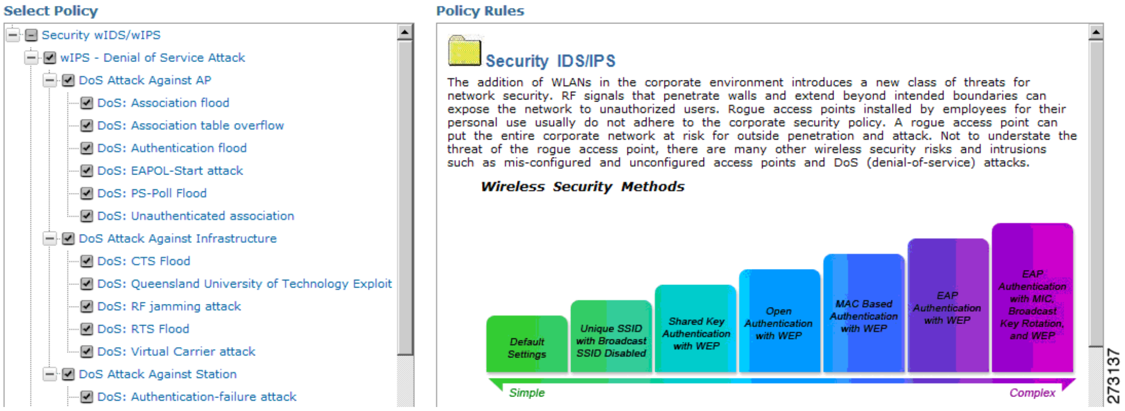


□ Name	SSID List
□ Any	-
□ Guest	-
□ MyWLAN	SSID1 SSID2 SSID3
□ Neighbor	-
□ Other	-

d. Click **Next**.

The Select Policy and Policy Rules summary window appears (see Figure 6-11).

Figure 6-11 Next > Select Policy Summary Window



Select Policy

- ☐ Security wIDS/wIPS
  - ☑ wIPS - Denial of Service Attack
    - ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow
      - ☑ DoS: Authentication flood
      - ☑ DoS: EAPOL-Start attack
      - ☑ DoS: PS-Poll Flood
      - ☑ DoS: Unauthenticated association
    - ☑ DoS Attack Against Infrastructure
      - ☑ DoS: CTS Flood
      - ☑ DoS: Queensland University of Technology Exploit
      - ☑ DoS: RF jamming attack
      - ☑ DoS: RTS Flood
      - ☑ DoS: Virtual Carrier attack
    - ☑ DoS Attack Against Station
      - ☑ DoS: Authentication-failure attack

Policy Rules

Security IDS/IPS

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.

Wireless Security Methods

Default Settings
Unique SSID with Broadcast SSID Disabled
Shared Key Authentication with WEP
Open Authentication with WEP
MAC Based Authentication with WEP
EAP Authentication with WEP
EAP Authentication with MIC, Broadcast Key Rotation, and WEP
Simple
Complex
273137

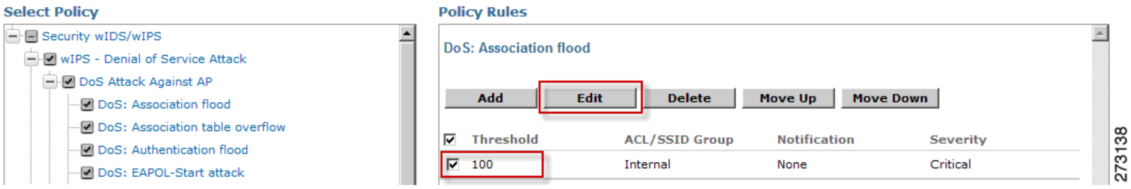
Note At the policy window (Figure 6-11), you can enable or disable attacks to be detected and reported. You can also edit specific thresholds for alarms and turn on forensics.

Step 7 To enable or disable attacks to be detected and reported, check the check box next to the specific attack type in question (left panel).

Step 8 To edit the profile, click on the name of the attack type (such as DoS: Association Flood).

The configuration panel for that attack type appears in the right panel above the policy rule description (see Figure 6-12).

Figure 6-12 Policy Rules Panel



Select Policy

- ☐ Security wIDS/wIPS
  - ☑ wIPS - Denial of Service Attack
    - ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow
      - ☑ DoS: Authentication flood
      - ☑ DoS: EAPOL-Start attack

Policy Rules

DoS: Association flood

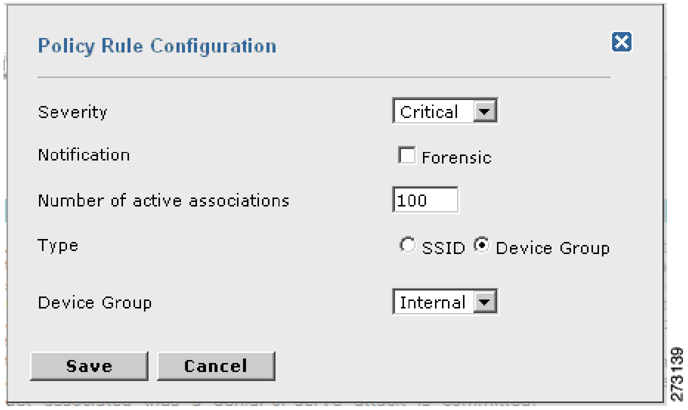
☑	Threshold	ACL/SSID Group	Notification	Severity
☑	100	Internal	None	Critical

Step 9 To modify a policy rule do the following:

a. Check the check box next to the policy rule and click **Edit**.

The Policy Rule Configuration window appears (see Figure 6-13).

Figure 6-13 Policy Rule Configuration Panel



Policy Rule Configuration

Severity: Critical

Notification: □ Forensic

Number of active associations: 100

Type: ○ SSID ● Device Group

Device Group: Internal

b. Select the severity of the alarm.

c. Check the forensic check box if you want to capture packets for this alarm.

d. Modify the number of active associations, if desired. (This value varies by alarm type).

e. Select the type of WLAN infrastructure (SSID or Device Group) that the system will monitor for attacks.

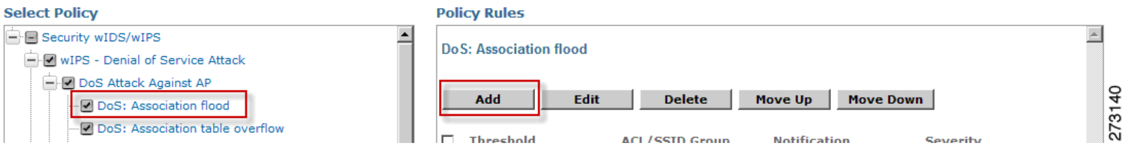
1. If you select SSID, continue with Step 10.
2. If you select Device Group, continue with Step 11.

Note **Device Group** (Type) and **Internal** are the defaults. *Internal* indicates all access points within the same RF Group. Selecting SSID as the type, allows you to monitor a separate network which is typical of an overlay deployment.

Step 10 (Optional, overlay deployments only) To add a policy rule for an SSID, do the following:

a. To add a policy rule, click **Add** (see Figure 6-14).

Figure 6-14 Adding a Policy Rule



Select Policy

- ☑ Security wIDS/wIPS
  - ☑ wIPS - Denial of Service Attack
    - ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow

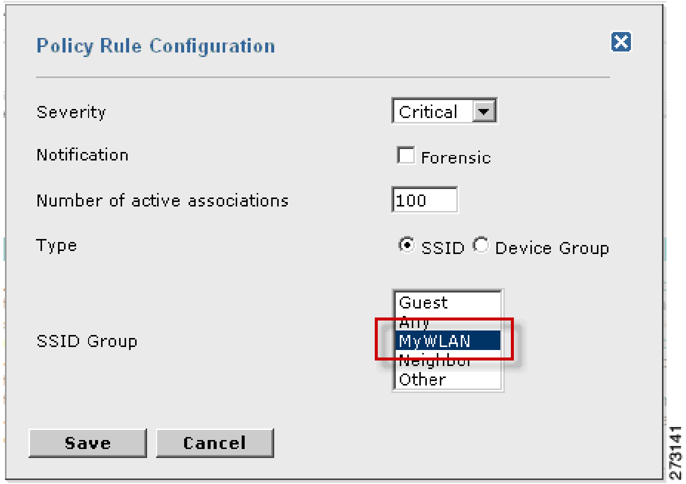
Policy Rules

DoS: Association flood

b. In the policy rule configuration panel that appears, select **MyWLAN** from the SSID Group pull-down menu (see Figure 6-15).

Note SSID is already selected as the type.

Figure 6-15 Policy Configuration Panel for SSIDs



Policy Rule Configuration

Severity	Critical ▾
Notification	☐ Forensic
Number of active associations	100
Type	● SSID ○ Device Group
SSID Group	Guest Any MyWLAN Neighbor Other

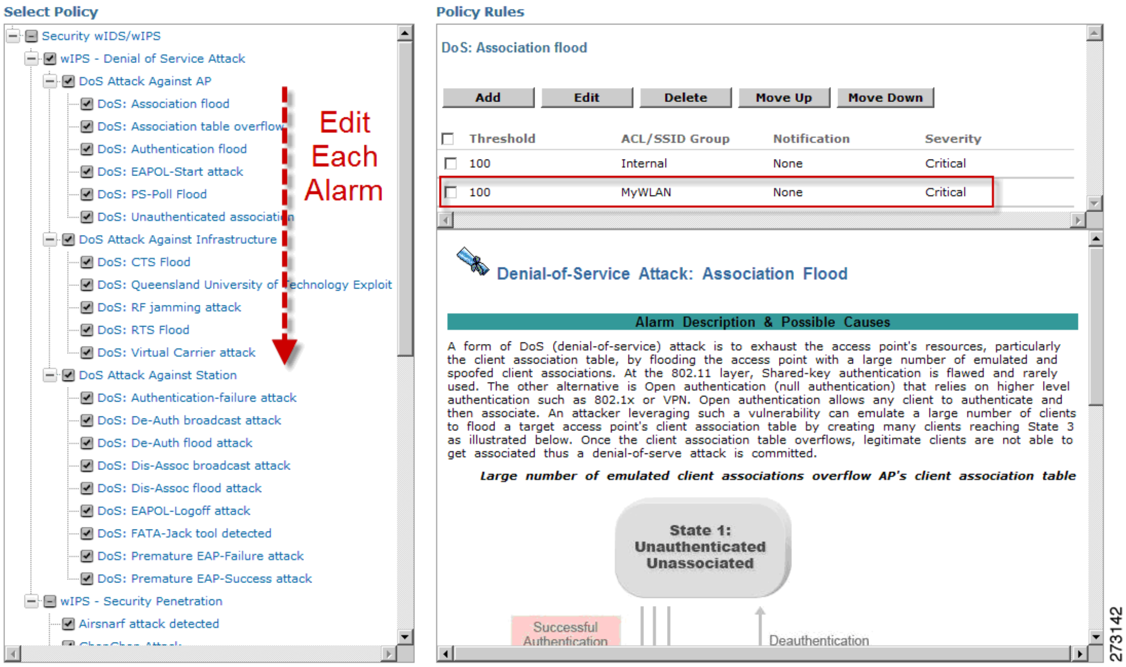
Save Cancel

c. Click **Save** after all changes are complete.

d. Modify each policy rule. Continue to Step 11 when all edits are complete.

Note When you configure a system to monitor another WLAN infrastructure by SSID, changes must be made for each and every policy rule to monitor by SSID. You must create a policy rule under each separate alarm which defines the system to monitor attacks against the SSID Group created earlier.

Figure 6-16 Edit Policy Rules for SSID Monitoring



Select Policy

- ☐ Security wIDS/wIPS
  - ☑ wIPS - Denial of Service Attack
    - ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow
      - ☑ DoS: Authentication flood
      - ☑ DoS: EAPOL-Start attack
      - ☑ DoS: PS-Poll Flood
      - ☑ DoS: Unauthenticated association
    - ☑ DoS Attack Against Infrastructure
      - ☑ DoS: CTS Flood
      - ☑ DoS: Queensland University of Technology Exploit
      - ☑ DoS: RF jamming attack
      - ☑ DoS: RTS Flood
      - ☑ DoS: Virtual Carrier attack
    - ☑ DoS Attack Against Station
      - ☑ DoS: Authentication-failure attack
      - ☑ DoS: De-Auth broadcast attack
      - ☑ DoS: De-Auth flood attack
      - ☑ DoS: Dis-Assoc broadcast attack
      - ☑ DoS: Dis-Assoc flood attack
      - ☑ DoS: EAPOL-Logoff attack
      - ☑ DoS: FATA-Jack tool detected
      - ☑ DoS: Premature EAP-Failure attack
      - ☑ DoS: Premature EAP-Success attack
  - ☑ wIPS - Security Penetration
    - ☑ Airsnarf attack detected

Policy Rules

DoS: Association flood

Add Edit Delete Move Up Move Down

☐	Threshold	ACL/SSID Group	Notification	Severity
☐	100	Internal	None	Critical
☐	100	MyWLAN	None	Critical

Denial-of-Service Attack: Association Flood

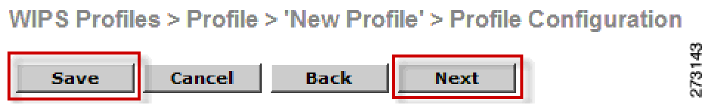
Alarm Description & Possible Causes

A form of DoS (denial-of-service) attack is to exhaust the access point's resources, particularly the client association table, by flooding the access point with a large number of emulated and 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 leveraging such a vulnerability can emulate a large number of clients to flood a target access point's client association table by creating many clients reaching State 3 as illustrated below. Once the client association table overflows, legitimate clients are not able to get associated thus a denial-of-serve attack is committed.

Large number of emulated client associations overflow AP's client association table

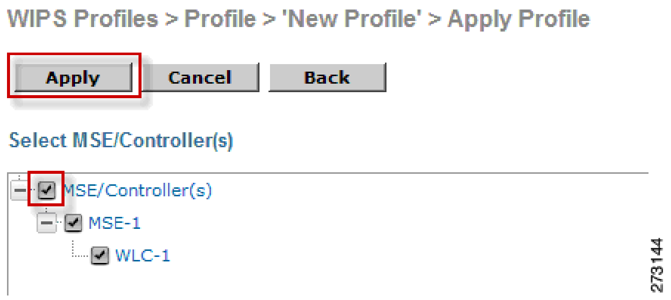
Step 11 Click **Save** to save the Profile (SSID or Device Group). Click **Next** (see Figure 6-17).

Figure 6-17 Saving Profile Configuration


WIPS Profiles > Profile > 'New Profile' > Profile Configuration
Save
Cancel
Back
Next
273143

Step 12 Select the MSE/Controller combinations to apply the profile to and then click **Apply** (see Figure 6-18).

Figure 6-18 Applying Profile Configuration.



☑ MSE/Controller(s)
☑ MSE-1
☑ WLC-1

CHAPTER 7

Monitoring the System and Services

This chapter describes how to monitor the mobility services engine by configuring and viewing alarms, events, and logs as well as how to generate reports on system use and element counts (tags, clients, rogue clients, and access points).

It also describes how to use Cisco WCS to monitor clients (wired and wireless), tags, chokepoints, and Wi-Fi TDOA receivers.

This chapter contains the following sections:

Working with Alarms

This section describes how to view, assign, and clear alarms and events on a mobility services engine using Cisco WCS. Details on how to have email notifications for alarms sent to you is described as well as how to define those types (all, critical, major, minor, warning) of alarm notifications that are sent to you.

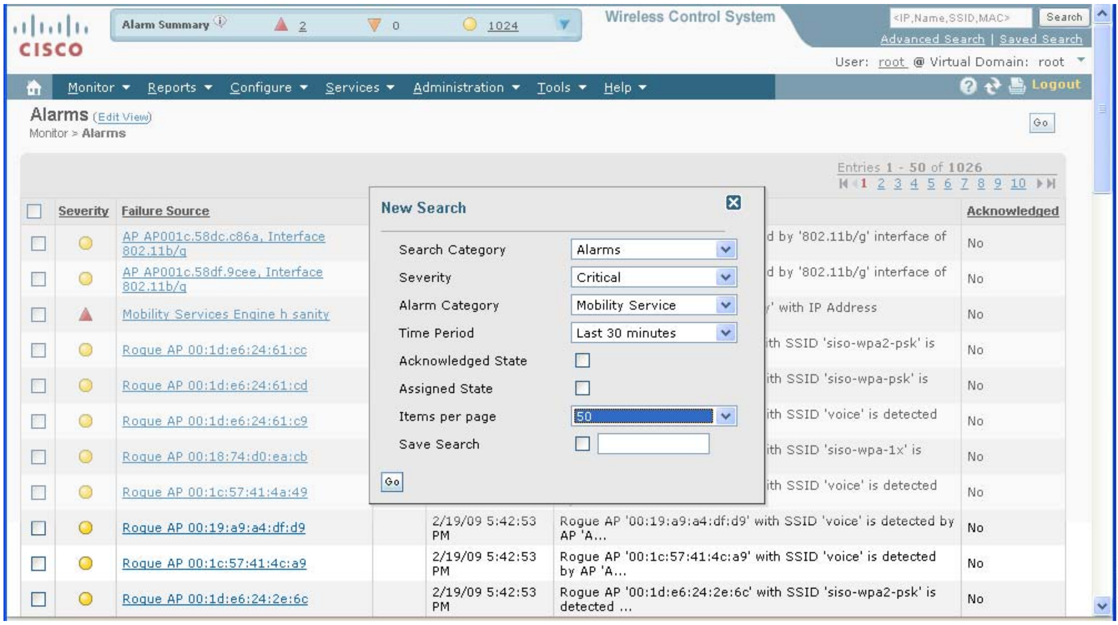
Viewing Alarms

To view mobility services engine alarms, follow these steps:

Step 1 In Cisco WCS, choose **Monitor > Alarms**.

Step 2 Click the **Advanced Search** link in the navigation bar (top-right). A configurable search panel for alarms appears (see Figure 7-1).

Figure 7-1 Advanced Search Alarm Panel



New Search

Search Category	Alarms
Severity	Critical
Alarm Category	Mobility Service
Time Period	Last 30 minutes
Acknowledged State	☐
Assigned State	☐
Items per page	50
Save Search	☐

Go

☐	Severity	Failure Source			Acknowledged
☐	●	AP AP001c.58dc.c86a, Interface 802.11b/g		d by '802.11b/g' interface of	No
☐	●	AP AP001c.58df.9cee, Interface 802.11b/g		d by '802.11b/g' interface of	No
☐	▲	Mobility Services Engine h sanity		' with IP Address	No
☐	●	Rogue AP 00:1d:e6:24:61:cc		ith SSID 'siso-wpa2-psk' is	No
☐	●	Rogue AP 00:1d:e6:24:61:cd		ith SSID 'siso-wpa-psk' is	No
☐	●	Rogue AP 00:1d:e6:24:61:c9		ith SSID 'voice' is detected	No
☐	●	Rogue AP 00:18:74:d0:ea:cb		ith SSID 'siso-wpa-1x' is	No
☐	●	Rogue AP 00:1c:57:41:4a:49		ith SSID 'voice' is detected	No
☐	●	Rogue AP 00:19:a9:a4:df:d9	2/19/09 5:42:53 PM	Rogue AP '00:19:a9:a4:df:d9' with SSID 'voice' is detected by AP 'A...	No
☐	●	Rogue AP 00:1c:57:41:4c:a9	2/19/09 5:42:53 PM	Rogue AP '00:1c:57:41:4c:a9' with SSID 'voice' is detected by AP 'A...	No
☐	●	Rogue AP 00:1d:e6:24:2e:6c	2/19/09 5:42:53 PM	Rogue AP '00:1d:e6:24:2e:6c' with SSID 'siso-wpa2-psk' is detected ...	No

Step 3 Select **Alarms** as the Search Category.

Step 4 Select the Severity of Alarms to display. Options are All Severities, Critical, Major, Minor, or Warning.

Step 5 Select **Mobility Service** from the Alarm Category.

Options are: All Types, Access Points, Controller, Coverage Hole, Config Audit, Mobility Service Location Notifications, Interference, Mesh Links, Rogue AP, Rogue Adhoc**,** Security and WCS.

Step 6 Select the time frame for which you want to review alarms from the Time Period drop-down menu.

Options range from minutes (5, 15 and 30) to hours (1 and 8) to days (1 and 7). To display all, select **Any time**.

Step 7 Check the **Acknowledged State** check box to exclude the acknowledged alarms and their count from the Alarm Summary window.

Step 8 Check the **Assigned Stat**e check box to exclude the assigned alarms and their count from the Alarm Summary window.

Step 9 Select the number of alarms to display on each window from the Items per page drop-down menu.

Step 10 To save the search criteria for later use, check the **Save Search** box and enter a name for the search.

Note You can initiate the search thereafter, by clicking the Saved Searches link at the top-right of the navigation bar.

Step 11 Click **Go**. Alarms summary panel appears with search results.

Note Click the column headings (Severity, Failure Object, Owner, Date/Time, and Message) to sort alarms.

Step 12 Repeat Step 2 to Step 11 to see notifications for access points by entering **Access Points** as the alarm category in Step 5.

Assigning and Unassigning Alarms

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

Step 1 Display the Alarms window as described in the "Viewing Alarms" section on page 7-2.

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

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

Step 3 From the Select a command drop-down menu, 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

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

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

Step 1 Display the Alarms window as described in the "Viewing Alarms" section on page 7-2.

Step 2 Select the alarms that you want to delete or clear by checking their corresponding check boxes.

Step 3 From the Select a command drop-down menu, choose **Delete** or **Clear**. Click **Go**.

Emailing Alarm Notifications

Cisco WCS lets you send alarm notifications to a specific email address. Sending notifications through email enables you to take prompt action when needed.

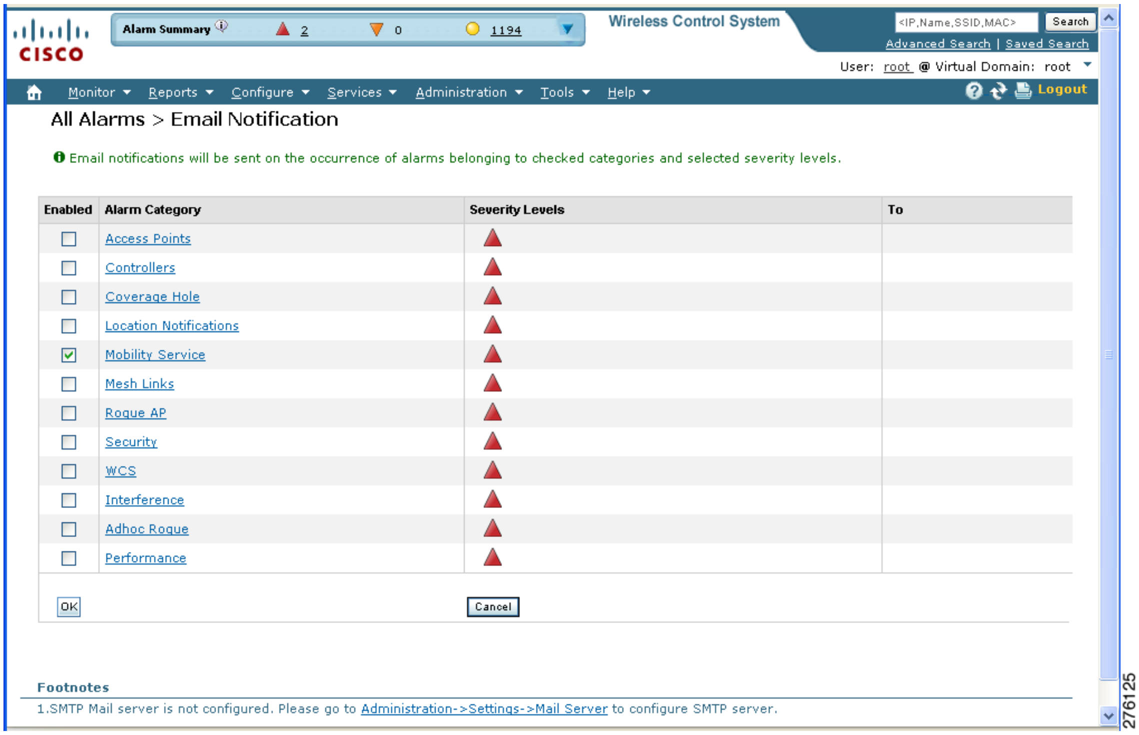
You can select the alarm severity types (critical, major, minor, and warning) you have emailed to you.

To send alarm notifications, follow these steps:

Step 1 Choose **Monitor > Alarms**.

Step 2 From the Select a commands drop-down menu, choose **Email Notification**. Click **Go**. The Email Notification window appears (see Figure 7-2).

Figure 7-2 All Alarms > Email Notification Window



All Alarms > Email Notification

Email notifications will be sent on the occurrence of alarms belonging to checked categories and selected severity levels.

Enabled	Alarm Category	Severity Levels	To
□	Access Points	▲	
□	Controllers	▲	
□	Coverage Hole	▲	
□	Location Notifications	▲	
☑	Mobility Service	▲	
□	Mesh Links	▲	
□	Rogue AP	▲	
□	Security	▲	
□	WCS	▲	
□	Interference	▲	
□	Adhoc Rogue	▲	
□	Performance	▲	

OK Cancel

Footnotes

1.SMTP Mail server is not configured. Please go to Administration->Settings->Mail Server to configure SMTP server.

Note A SMTP Mail Server must be defined prior to entry of target email addresses for email notification. Choose **Administration > Settings > Mail Server Configuration** to enter the appropriate information. You can also select the Administration > Settings > Mail Server link, if displayed, on the Email Notification window noted above.

Step 3 Click the **Enabled** box next to the **Mobility Service**.

Note Enabling the **Mobility Service** alarm category sends all alarms related to the mobility services engine and the location appliance to the defined email address.

Step 4 Click the **Mobility Service** link. The window for configuring the alarm severity types that are reported for the mobility services engine appears.

Step 5 Check the check box next to all the alarm severity types for which you want email notifications sent.

Step 6 In the To field, enter the email address or addresses to which you want the email notifications sent. Separate email addresses by commas.

Step 7 Click **OK**.

The Alarms > Notification window appears. The changes to the reported alarm severity levels and the recipient email address for email notifications are displayed.

Working with Events

You can use Cisco WCS to view mobility services engine and location notification events. You can search and display events based on their severity (critical, major, minor, warning, clear, info) and event category.

You can search by the following event categories:

- By network coverage: coverage holes and interference
- By link: mesh links
- By notifications: location notifications
- By product type: access points (rogue and non-rogue), clients, controllers, and mobility service

Note The product type: mobility service reports events for mobility services engines.

- By security

Additionally, you can search for an element's events 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 Cisco WCS, choose **Monitor > Events**.

Step 2 In the Events window:

- If you want to display the events for a specific element, and you know its IP address, name, WLAN SSID, or MAC address, enter that value in the Search field of the navigation bar (top-right). Click **Search.**
- To display events by severity and category, click **Advanced Search** in the navigation bar and select the appropriate options from the Severity and Event Category drop-down menus. Click **Go**.

Step 3 If Cisco WCS 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.

Working with Logs

This section describes how to configure logging options and how to download log files.

Configuring Logging Options

You can use Cisco WCS to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to configure.

Step 3 Choose **System > Advanced Parameters**. The advanced parameters for the selected mobility services engine appears.

Step 4 Scroll down to the Logging Options section and choose the appropriate option from the Logging Level drop-down menu.

There are four logging options: **Off**, **Error**, **Information**, and **Trace**.

Caution Use **Error** and **Trace** only when directed to do so by Cisco Technical Assistance Center (TAC) personnel.

Step 5 Check the **Enabled** check box next to each element listed in that section to begin logging of its events.

Step 6 Click **Save**.

Downloading Log Files

If you need to analyze mobility services engine log files, you can use Cisco WCS to download them to your system. Cisco WCS downloads a zip file containing the log files.

To download a zip file containing the log files, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine to view its status.

Step 3 Choose **System > Logs** (left panel).

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.

Generating Reports

In Cisco WCS, you can generate a device utilization and location utilization report for a mobility services engine. By default, reports are stored on the Cisco WCS server.

Once you define the report criteria, you can save the device and location utilization reports for future diagnostic use and run them on either an ad hoc or scheduled basis.

You can define the following criteria for a device utilization report:

- Which mobility services engine or engines to monitor
- How often the report is generated
- How the data is graphed on the charts
- Whether the report is emailed or exported to a file

You can view the following in a location utilization report:

- Chart 1 summarizes and graphs CPU and memory utilization
- Chart 2 summarizes and graphs client count, tag count, rogue client count, rogue access point count, and ad hoc rogue count

Creating a Device Utilization Report

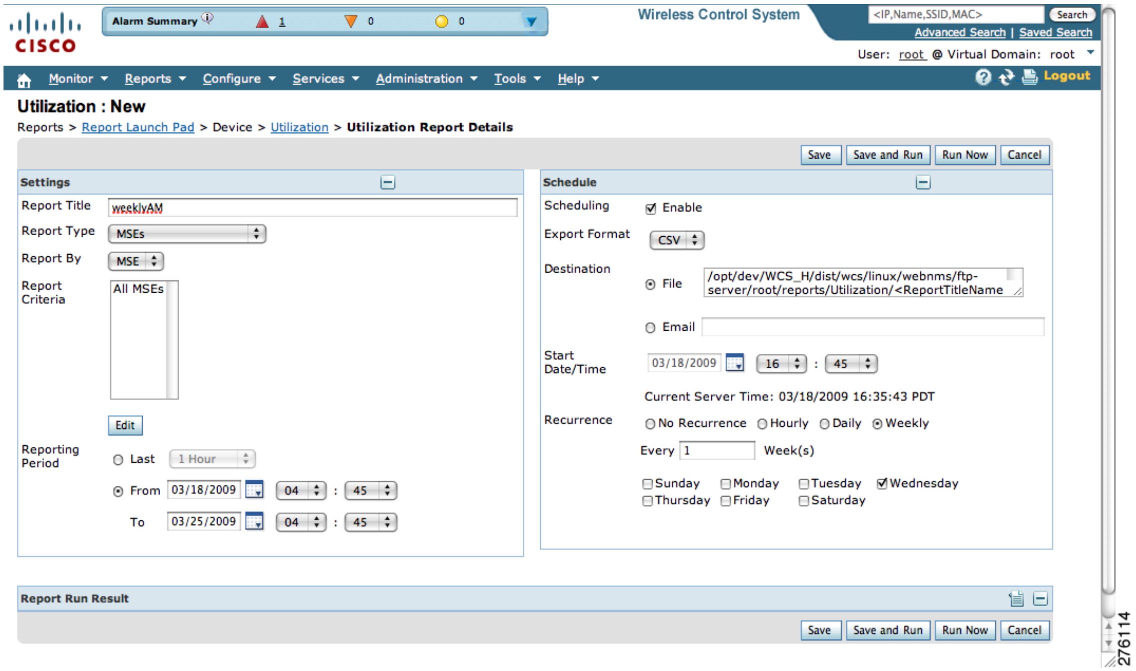
To create a utilization report for the mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Reports > Report Launch Pad**.

Step 2 Choose **Device > Utilization**.

Step 3 Click **New**. The Utilization: New window appears (see Figure 7-3).

Figure 7-3 Device > Utilization New Window



Utilization : New

Reports > Report Launch Pad > Device > Utilization > Utilization Report Details

Save | Save and Run | Run Now | Cancel

Settings

Report Title: weeklyAM

Report Type: MSEs

Report By: MSE

Report Criteria: All MSEs

Edit

Reporting Period: ○ Last 1 Hour; ● From 03/18/2009 04 : 45 To 03/25/2009 04 : 45

Schedule

Scheduling: ☑ Enable

Export Format: CSV

Destination: ● File /opt/dev/WCS_H/dist/wcs/linux/webnms/ftp-server/root/reports/Utilization/<ReportTitleName; ○ Email

Start Date/Time: 03/18/2009 16 : 45

Current Server Time: 03/18/2009 16:35:43 PDT

Recurrence: ○ No Recurrence ○ Hourly ○ Daily ● Weekly

Every 1 Week(s)

☐ Sunday ☐ Monday ☐ Tuesday ☑ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

Report Run Result

Save | Save and Run | Run Now | Cancel

Step 4 In the settings panel, enter a report title.

Step 5 The Report Type and Report By selections are always MSE.

Step 6 Click **Edit** to select either a specific mobility services engine or **All MSEs** from the pop-up panel that appears.

Step 7 Enter the reporting period. You can define the report to collect data hourly, weekly, or at a specific date and time. The selected reporting period type will display on the x-axis.

Note The reporting period uses a 24-hour rather than a 12-hour clock. For example, select hour 13 for 1:00 p.m.

Step 8 In the Schedule panel (right), check the **Enable Schedule** check box.

Step 9 Select the report format (CSV or PDF) from the Export Report drop-down menu.

Step 10 Select either **File** or **Email** as the destination of the report.

- If you select the File option, a destination path must first be defined at the **Administration > Settings** > *Report* window. Enter the destination path for the files in the Repository Path field.
- If you select the Email option, an SMTP Mail Server must be defined prior to entry of target email address. Choose **Administrator > Settings >** *Mail Server Configuration* to enter the appropriate information.

Step 11 Enter a start date (MM:DD:YYYY) or click the calendar icon to select a date.

Step 12 Specify a start time using the hour and minute drop-down menus.

Step 13 Click one of the Recurrence buttons to select how often the report is run.

Note The days of the week appear on the screen only when the weekly option is chosen.

Step 14 When finished with all of the above steps, do one of the following:

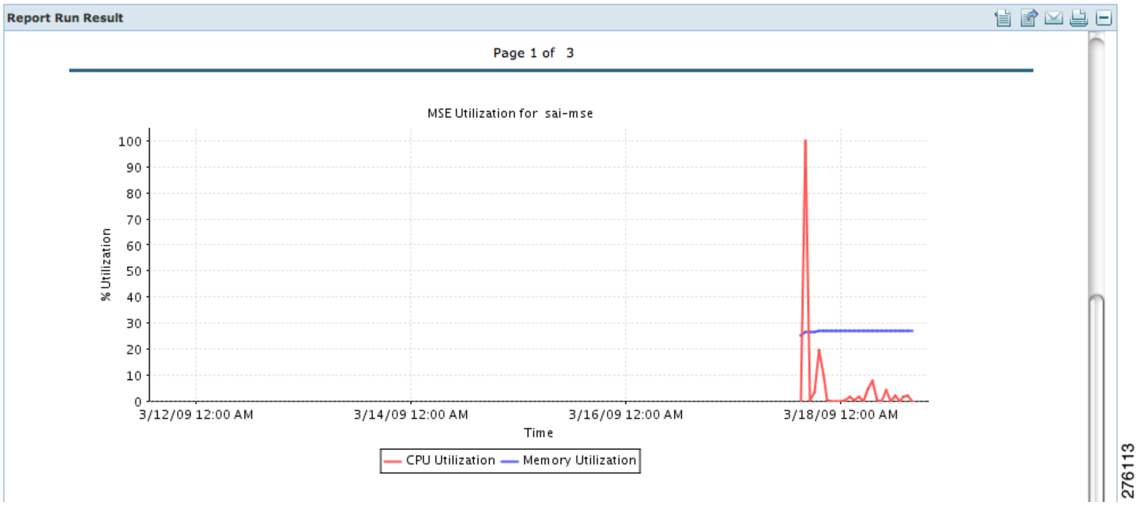
- Click **Save** to save edits. The report is run at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule panel.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any pending, scheduled run of that report. Results appear the bottom of the window. The report also runs at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule panel.
  - At the results window, click **Cancel** to cancel the defined report.
- Click **Run Now** if you want to run the report immediately and review the results in the WCS window. The report runs regardless of any pending, scheduled run of that report. Results appear at the bottom of the window. Click **Save** if you want to save the report criteria you entered.

Note You can also use the **Run Now** command to check the defined report criteria before saving it or to run reports as necessary.

The results appear at the bottom of the window (see Figure 7-3).

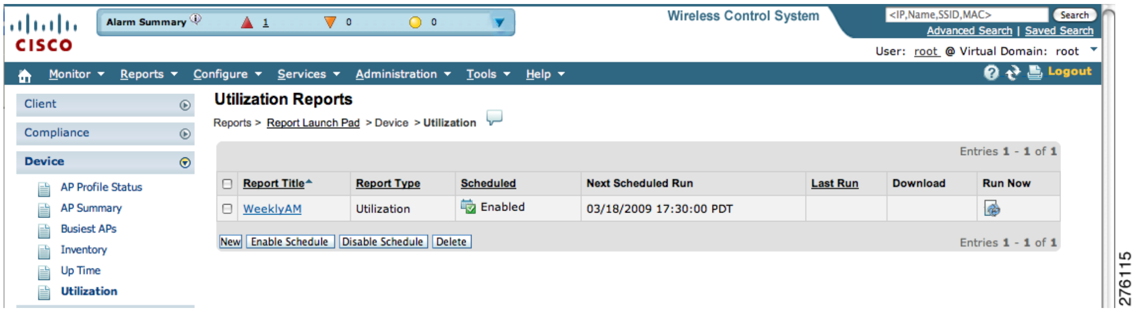
Note Only the CPU and memory utilization reports as shown in the example below (see Figure 7-4).

Figure 7-4 Device > MSE Utilization > Results



Step 15 If you selected the Save or Save and Run option, click either **Reports > Saved Reports** (or **Reports > Scheduled Runs** if it has not yet run and is scheduled to run). The Utilization Reports summary window appears (see Figure 7-5).

Figure 7-5 Utilization Reports Summary Window



Utilization Reports

Reports > Report Launch Pad > Device > Utilization

Entries 1 - 1 of 1

□	Report Title	Report Type	Scheduled	Next Scheduled Run	Last Run	Download	Run Now
□	WeeklyAM	Utilization	Enabled	03/18/2009 17:30:00 PDT			

Entries 1 - 1 of 1

If the report is scheduled, it is shown as enabled and the next scheduled run date is noted.

If the report has run and is not scheduled to run again, it is shown as expired.

If the report has run and is scheduled to run again, it is shown as disabled.

Step 16 To enable, disable, or delete a report, check the check box next to the report title and click the appropriate button.

Viewing Saved Utilization Report

To download a saved report, follow these steps:

Step 1 In Cisco WCS, choose **Reports > Saved Reports**.

Step 2 Click the **Download** icon for your request. It is downloaded and saved in the defined directory or emailed.

Viewing Scheduled Utilization Runs

To review status for a scheduled report, follow these steps:

Step 1 In Cisco WCS, choose **Reports > Scheduled Runs**.

Step 2 Click the **History** icon to see the date of the last report run.

Step 3 Click the **Download** icon for your report. It is downloaded and saved in the defined directory or emailed.

Security Reports and Alarms for wIPS

You can view, modify, or create a security report or alarm for wIPS.

Note Security reports do not show the status of autonomous access points.

The choices are as follows:

- Adaptive wIPS Alarms—Alarms reported for wIPS on monitor mode access points.
- Adaptive wIPS Top 10 AP—Lists the last 10 events reported for monitor access points.
- Adhoc Rogue Event—Displays all adhoc events that WCS has received in the selected timeframe.
- Adhoc Rogues—Displays all adhocs that have been updated in the selected timeframe.
- New Rogue APs—Displays, in tabular form, all rogues detected in a selected timeframe. It provides which new rogues were detected within a selected time. The created time indicates the time at which the rogue was first detected.
- New Rogue AP Count—Displays, in graphical form, all rogues detected in a selected timeframe.
- Rogue APs—Displays all rogues that are active in your network and have been updated in the selected timeframe. WCS receives updated events for rogues that are detected
- Rogue APs Event—Displays all the events received by WCS. The controller sends updates of detected rogues if any of the attributes change or new rogues are detected.

Note This report was formally called the Rogue Detected by AP.

- Security Summary—Shows the number of association failures, rogues access points, ad hocs, and access point connections or disconnections over one month.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any scheduled time associated with the report and is viewable in the **Results** tab. Additionally, the report is run at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule tab.
  - At the results window, you can cancel or delete the report.

Creating a New wIPS Security or Alarms Report

Security reports provide a number of details on access points and rogue access points for wIPS.

To create a new security report, follow these steps:

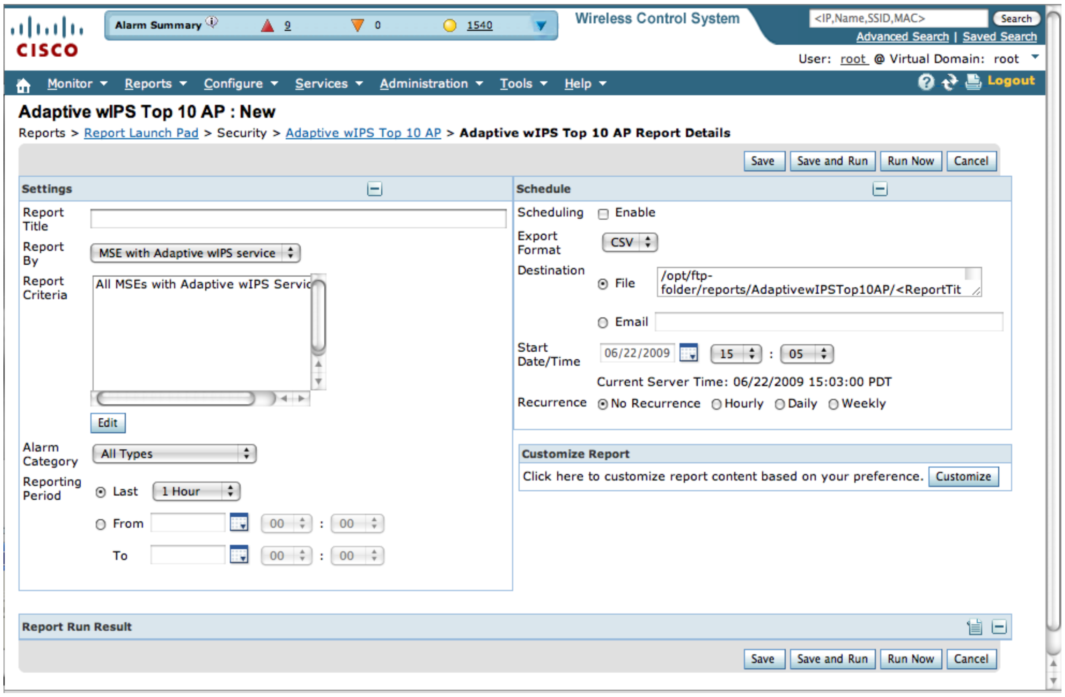
Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Report Launch Pad**. The Report Launch Pad window appears.

Step 2 Choose **Security** (left panel) and click on one of the report types in the left panel (such as Adaptive wIPS Top 10 Report Details).

Step 3 Click **New**. The new report window appears (see Figure 7-6)

Figure 7-6   New Report Window



Adaptive wIPS Top 10 AP : New

Reports > Report Launch Pad > Security > Adaptive wIPS Top 10 AP > **Adaptive wIPS Top 10 AP Report Details**

Settings

Report Title:

Report By: MSE with Adaptive wIPS service

Report Criteria: All MSEs with Adaptive wIPS Servic

Alarm Category: All Types

Reporting Period: ● Last 1 Hour
○ From 00 : 00
To 00 : 00

Schedule

Scheduling: □ Enable

Export Format: CSV

Destination: ● File /opt/ftp-folder/reports/AdaptivewIPSTop10AP/<ReportTit
○ Email

Start Date/Time: 06/22/2009 15 : 05

Current Server Time: 06/22/2009 15:03:00 PDT

Recurrence: ● No Recurrence ○ Hourly ○ Daily ○ Weekly

Customize Report

Click here to customize report content based on your preference.

Step 4 In the settings panel, enter a report title.

Step 5 The Report By selections is always **MSE with Adaptive wIPS Service**.

Step 6 The Report Criteria is always either a specific mobility services engine or **All MSEs with Adaptive wIPS Service**

Step 7 Click **Edit** to add or modify the Report Crieteria. A pop-up panel appears.

Step 8 Enter the reporting period. You can define the report to collect data hourly, weekly, or at a specific date and time. The selected reporting period type will display on the x-axis.

Note The reporting period uses a 24-hour rather than a 12-hour clock. For example, select hour 13 for 1:00 p.m.

Step 9 In the Schedule panel (right), check the **Enable Schedule** check box.

Step 10 Select the report format (CSV or PDF) from the Export Report drop-down menu.

Step 11 Select either **File** or **Email** as the destination of the report.

- If you select the File option, a destination path must first be defined at the **Administration > Settings** > *Report* window. Enter the destination path for the files in the Repository Path field.
- If you select the Email option, an SMTP Mail Server must be defined prior to entry of target email address. Choose **Administrator** > **Settings** > *Mail Server Configuration* to enter the appropriate information.

Step 12 Enter a start date (MM:DD:YYYY) or click the calendar icon to select a date.

Step 13 Specify a start time using the hour and minute drop-down menus.

Step 14 Click one of the Recurrence buttons to select how often the report is run.

Note The days of the week only appear on the when the weekly option is chosen.

Step 15 When finished with all of the above steps, do one of the following:

- Click **Save** to save edits. The report is run at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule panel.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any pending, scheduled run of that report. Results appear the bottom of the window. The report also runs at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule panel.
  - At the results window, click **Cancel** to cancel the defined report.
- Click **Run Now** if you want to run the report immediately and review the results in the WCS window. The report runs regardless of any pending, scheduled run of that report. Results appear at the bottom of the window. Click **Save** if you want to save the report criteria you entered.

Note You can also use the **Run Now** command to check the defined report criteria before saving it or to run reports as necessary.

The results appear at the bottom of the window.

Step 16 Repeat Step 2 to Step 15 for each wIPS report you want to create.

Viewing Saved wIPS Report

To download a saved report, follow these steps:

Step 1 In Cisco WCS, choose **Reports > Saved Reports**.

Step 2 Click the **Download** icon for your request. It is downloaded and saved in the defined directory or emailed.

Viewing Scheduled wIPS Report Runs

To review status for a scheduled report, follow these steps:

Step 1 In Cisco WCS, choose **Reports > Scheduled Runs**.

Step 2 Click the **History** icon to see the date of the last report run.

Step 3 Click the **Download** icon for your report. It is downloaded and saved in the defined directory or emailed.

CHAPTER 8

Performing Maintenance Operations

This chapter describes how to back up and restore mobility services engine data and how to update the mobility services engine software. It also describes other maintenance operations.

This chapter contains the following sections:

- Recovering a Lost Password, page 8-2
- Recovering a Lost Root Password, page 8-2
- Downloading Software to Mobility Services Engines, page 8-4
- Downloading Software to Mobility Services Engines, page 8-4
- Configuring NTP Server, page 8-6
- System Reset, Defragmenting Database and Clearing Database, page 8-6

Recovering a Lost Password

To recover a lost or forgotten password for a mobility services engine, follow these steps:

Step 1 When the GRUB screen comes up, press **Esc** to enter the boot menu.

Step 2 Press **e** to edit.

Step 3 Navigate to the line beginning with *kernel* and press **e.**

At the end of the line put a space, followed by the number one (**1**). Press **Enter** to save this change.

Step 4 Press **b** to begin boot.

The boot sequence will commence and at the end the user will be given a shell prompt.

Step 5 The user may change the root password by invoking the **passwd** command.

Step 6 Enter and confirm the new password.

Step 7 Reboot the machine.

Recovering a Lost Root Password

To recover a lost or forgotten root password for a mobility services engine, follow these steps:

Step 1 When the GRUB screen comes up, press **Esc** to enter the boot menu.

Step 2 Press **e** to edit.

Step 3 Navigate to the line beginning with *kernel* and press **e.**

At the end of the line enter a space and the number one (**1**). Press **Enter** to save this change.

Step 4 Press **b** to begin boot sequence.

At the end of the boot sequence, a shell prompt appears.

Note The shell prompt does not appear if you have setup a single user mode password.

Step 5 You can change the root password by entering the **passwd** command.

Step 6 Enter and confirm the new password.

Step 7 Restart the machine.

Backing Up and Restoring Mobility Services Engine Data

This information describes how to back up and restore mobility services engine data. It also describes how to enable automatic backup.

Backing Up Mobility Services Engine Historical Data

Cisco WCS includes functionality for backing up mobility services engine data.

Note You cannot run the backup process in the background while working on other mobility services engine operations in other Cisco WCS windows.

To back up mobility services engine data, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services.**

Step 2 Click the name of the mobility services engine that you want to back up.

Step 3 Choose **System > Maintenance > Backup** (left panel).

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 Cisco WCS.

Status of the backup can be seen on the screen while the backup is in process. Three items will display on the screen 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 Backups are stored in the FTP directory you specify during the Cisco WCS installation.

Restoring Mobility Services Engine Historical Data

You can use Cisco WCS to restore backed-up historical data.

Note You cannot run the restore process in the background while working on other mobility service engine operations in other Cisco WCS windows.

To restore mobility services engine data, follow these steps:

Step 1 In Cisco WCS, choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to restore.

Step 3 Click **System > Maintenance > Restore** (left panel).

Step 4 Choose the file to restore from the drop-down menu.

Step 5 Enter the time in seconds after which restoration times out.

Step 6 Click **Submit** to start the restoration process.

Step 7 Click **OK** to confirm that you want to restore the data from the Cisco WCS server hard drive. When restoration is completed, Cisco WCS displays a message to that effect.

Enabling Automatic Data Backup

You can configure Cisco WCS to perform automatic backups of mobility services engine data on a regular basis.

To enable automatic backup of data on a mobility services engine, follow these steps:

Step 1 In Cisco WCS, choose **Administration > Background Tasks**.

Step 2 Check the **Mobility Service Backup** check box and click on its link.

Step 3 In the window that appears, check the **Enabled** check box.

Step 4 Modify the Max backups to keep field if you want to keep backup data more than 7 days (default).

Step 5 Modify the Interval field if you want the backup run more often or less often than 7 days (default).

Step 6 Click **Submit**.

The backups are stored in the FTP directory that you specify during the Cisco WCS installation.

Downloading Software to Mobility Services Engines

To download software to a mobility services engine, follow these steps:

Step 1 Verify that you can ping the mobility services engine from the Cisco WCS server or an external FTP server, whichever you are going to use for the application code download.

Step 2 In Cisco WCS, choose **Services > Mobility Services.**

Step 3 Click the name of the mobility services engine to which you want to download software.

Step 4 Choose **System > Maintenance > Download Software** (left panel).

Step 5 To download software, do one of the following:

- To download software listed in the Cisco WCS directory, choose **Select from uploaded images to transfer into the Server** from the drop-down menu. Then, choose a binary image from the drop-down menu.

  Cisco WCS downloads the binary images listed in the drop-down menu into the FTP server directory you have specified during the Cisco WCS installation.

- To use downloaded software available locally or over the network, select the **Browse a new software image to transfer into the Server** and click **Browse**. Locate the file and click **Open**.

Step 6 Enter the time in seconds (between 1 and 999999) after which software download times out.

Step 7 Click **Download** to send the software to the /opt/installers directory on the mobility services engine.

Step 8 After the image is transferred to the mobility services engine, log in to the mobility services engine CLI.

Step 9 Run the installer image from the */opt/installers* directory by entering the following command **./.bin** *mse image.* This installs the software.

Step 10 To run the software enter **/etc/init.d/msed start**.

Note To stop the software, enter **/etc/init.d/msed stop**, and to check status enter **/etc/init.d/msed status**.

Manually Downloading Software

If you do not want to automatically update the mobility services engine software using Cisco WCS, follow these steps to upgrade the software manually using a local (console) or remote (SSH) connection.

Step 1 Transfer the new mobility services engine image onto the hard drive.

a. Log in as root, and use the binary setting to send the image from an external FTP server root directory. The release note format is similar to the following and changes with each release: *CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz*.

Note The mobility services engine image is compressed at this point.

Note The default login name for the FTP server is *ftp-user*.

Your entries should look like this example:

```
# cd /opt/installers
# ftp <FTP Server IP address>
Name: <login>
Password: <password>
binary
get CISCO-MSE-L-K9-x-x-x-x-0-64bit.bin.gz
<CTRL-Z>
#
```

b. Verify that the image (*CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz*) is in the mobility services engine /opt/installers directory.

c. To decompress (unzip) the image file enter the following command:

gunzip *CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz*

The decompression yields a *bin* file.

d. Make sure that the *CISCO-MSE-L-K9-x-x-x-x.bin* file has execute permissions for the root user. If not, enter **chmod 755** *CISCO-MSE-L-K9-x-x-x-x.bin*.

Step 2 Manually stop the mobility services engine.

a. Log in as root and enter **/etc/init.d/msed stop**.

Step 3 Enter **/opt/installers/***CISCO-MSE-L-K9-x-x-x-x.bin* to install the new mobility services engine image.

Step 4 Start the new mobility services engine software by entering the following command:

/etc/init.d/msed start

Caution Only complete the next step that uninstalls the script files, if the system instructs you to do so. Removing the files unnecessarily erases your historical data.

Step 5 Enter **/opt/mse/uninstall** to uninstall the mobility services engine's script files.

Configuring NTP Server

You can configure NTP servers to set up the time and date of the mobility services engine.

Note

- You are automatically prompted to enable NTP and enter NTP server IP addresses as part of the automatic installation script for the mobility services engine. For more details on the automatic installation script, refer to the *Cisco 3350 Mobility Services Engine Getting Started Guide* or *Cisco 3310 Mobility Services Engine Getting Started Guide* at the following link: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html
- If you need to add or change an NTP server installation after a mobility services engine install, rerun the automatic installation script. You can configure the NTP server without adjusting the other values by just tabbing through the script.

Note For more information on NTP server configuration, consult the Linux configuration guides.

System Reset, Defragmenting Database and Clearing Database

For information on:

- Defragmenting the mobility services engine database
- Rebooting or shutting down the mobility services engine hardware
- Clearing the database file

Refer to the "Initiating Advanced Commands" section on page 4-11 of this configuration manual.