Cisco Wireless Intrusion Prevention System Configuration Guide, Release 8.0

First Published: July 31, 2013

Last Modified: July 28, 2014

CONTENTS

Preface

This preface describes the audience, organization, and conventions of the Cisco Wireless Intrusion Prevention System Configuration Guide. It also provides information on how to obtain other documentation. This chapter includes the following sections:

Audience

This guide is for administrators who configure and manage Wireless Intrusion and Prevention System (wIPS). Before you begin, you should be familiar with network structure, terms, and concepts.

Related Documentation

For more information on mobility services engine setup and installation, see the Cisco 3350 or 3355 Mobility Services Engine Getting Started Guide. These documents are available on Cisco.com at the following URL:

Click this link to browse to user documentation for the Cisco Unified Wireless Network solution:

http://www.cisco.com/en/US/products/ps9742/tsd_products_support_install_and_upgrade.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

P A R T █

Cisco MSE Prime Infrastructure User Interface

C H A P T E R 1

Overview

This chapter describes the role of the Cisco Mobility Services Engine (MSE) and the Cisco Wireless Intrusion Prevention System (wIPS) within the overall Cisco Unified Wireless Network (CUWN).

Cisco wIPS protects the network from penetration attacks, rogue wireless devices, and denial-of-service (DoS) attacks to improve security and meet compliance objectives. It offers flexible and scalable wireless network security for dedicated monitoring and detection of wireless network anomalies, unauthorized access, and RF attacks. This solution delivers integrated visibility and control access across the network, without the need for an overlay solution.

This chapter contains the following sections:

Information About wIPS

The Cisco Wireless Intrusion Prevention System 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 the CUWN and leveraging the efficiencies of Cisco Motion, wIPS is deployment-hardened and enterprise-ready. The wIPS is made up of the following components that work together to provide a unified security monitoring solution:

- A Mobility Services Engine running wIPS software—Serves as the central point of alarm aggregation for all controllers and their respective wIPS monitor mode access points. Alarm information and forensic files are stored on the Mobility Services Engine for archival purposes.

- A wIPS monitor mode access point—Provides constant channel scanning with attack detection and forensic (packet capture) capabilities.

> **Note** Access Point with a third module needs a monitor mode wIPS license even if the AP is running in local mode.

- Enhanced Local mode access point—Provides wireless service to clients in addition to time-sliced rogue scanning.

- Cisco Wireless Security and Spectrum Intelligence (WSSI)—Helps you to avoid radio frequency (RF) interference so that you get better coverage and performance on your wireless network.

- 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.

- Cisco Prime Infrastructure—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. Prime Infrastructure is also used to view wIPS alarms, forensic, reporting, and to access the attack encyclopedia. This figure shows the wireless Intrusion Prevention System.

Figure 1: Wireless Intrusion Prevention System
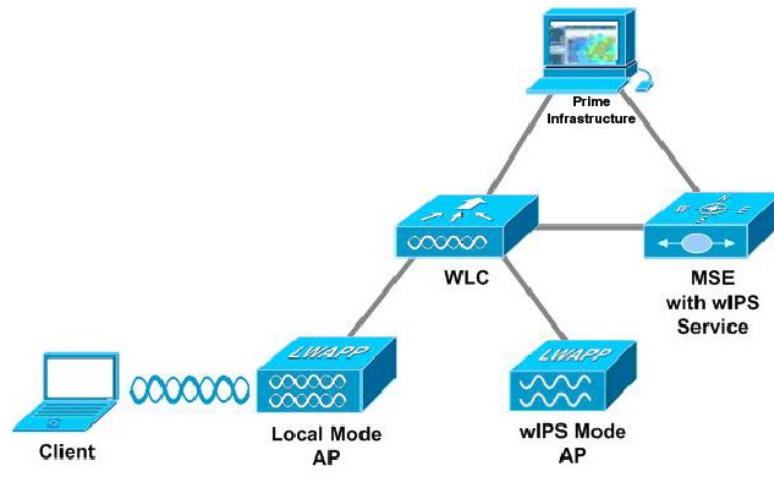
Communication among the system components involves the following protocols:

- 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 a 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 the Prime Infrastructure. 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 Prime Infrastructure. It is also employed to communicate rogue access point information from the controller to the Prime Infrastructure.

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).

This section contains the following topics:

- wIPS Integrated Within a Cisco Unified Wireless Network, on page 5
- wIPS Overlay Deployment in a Cisco Unified Wireless Network, on page 6
- wIPS Overlay in an Autonomous or Other Wireless Network, on page 7

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 Prime Infrastructure. We recommend this configuration because it allows the tightest integration between the client serving and monitoring infrastructure. This figure shows the integrated wIPS deployment within a Cisco wireless network.

Figure 2: wIPS Integrated Within CUWN
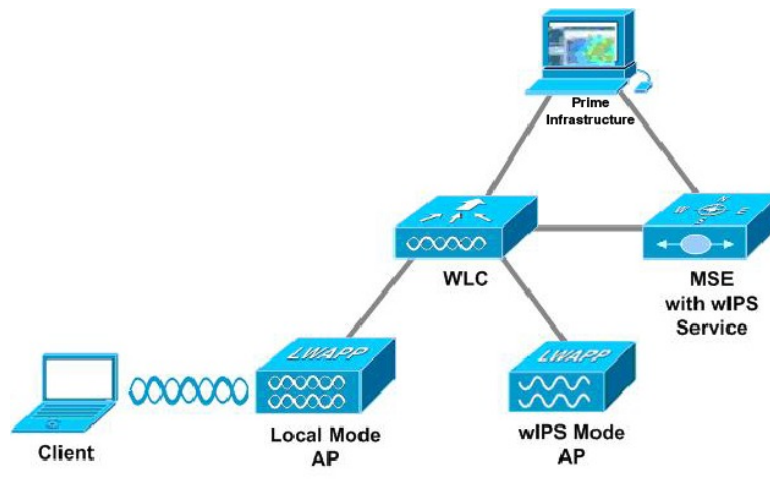
wIPS Overlay Deployment in a Cisco Unified Wireless Network

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 the Prime Infrastructure. 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. 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 the Prime Infrastructure. The below figure shows wIPS overlay deployment in a wireless network.

Figure 3: wIPS Overlay Monitoring Network Deployment in CUWN
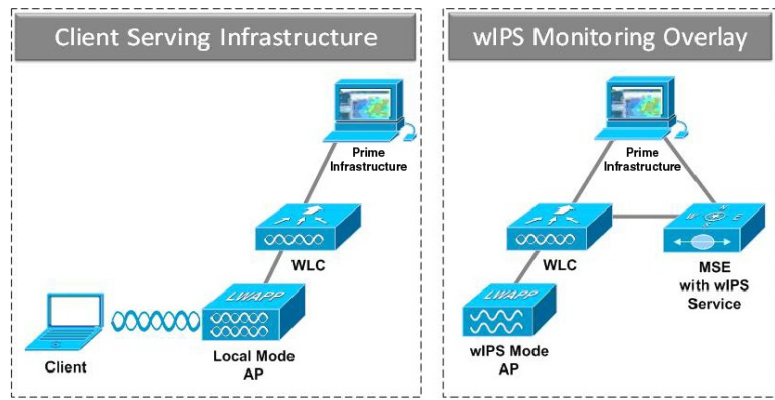
To configure the wIPS Overlay Monitoring network to provide security assessment of the client-serving infrastructure, specific configuration steps must be completed. The wIPS system operates on an assumption that only attacks against trusted devices must be logged. For an overlay system to view a separate Cisco Unified WLAN infrastructure as trusted, the controllers must be in the same RF Group.

Figure 4: Controller in Same RF Group for wIPS Overlay Monitoring Network
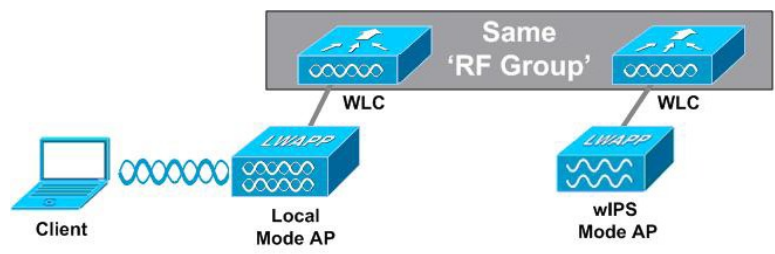
As a result of separating the client-serving infrastructure from the wIPS Overlay Monitoring Network, several monitoring caveats arise:

- wIPS alarms are only shown on the wIPS Overlay Prime Infrastructure instance.
- Management Frame Protection (MFP) alarms are only shown on the client infrastructure Prime Infrastructure instance.
- Rogue alarms are shown in both Prime Infrastructure instances.

- Rogue location accuracy is greater on the client-serving infrastructure Prime Infrastructure 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 Prime Infrastructure instances because some events such as wIPS only exist on the wIPS Overlay Prime Infrastructure. To monitor the comprehensive security of the wireless network, both security dashboard instances must be observed.

The below table summarizes some of the key differences between client-serving and overlay deployments.

Table 1: wIPS Client Serving and wIPS Monitoring Overlay Comparison

	Client-Serving Prime Infrastructure	wIPS Monitoring Overlay Prime Infrastructure
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, we recommend 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 an Autonomous or Other Wireless Network

The wIPS solution is also capable of performing security monitoring over an existing WLAN infrastructure other than CUWN. The application for this deployment is security monitoring of either Cisco autonomous access points or third-party access points.

This figure shows the wIPS overlay in an autonomous network.

Figure 5: wIPS Overlay in Autonomous Network
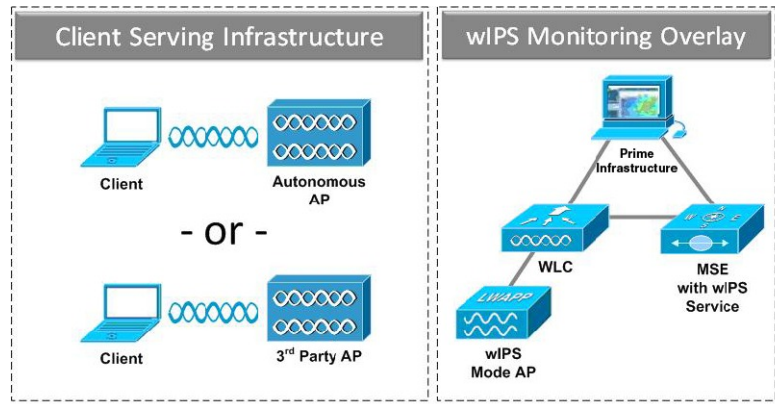
Differences Between Controller IDS and wIPS

This section contains the following topics:

Guidelines and Limitations

Forensics

We recommend that the forensics capability of the wIPS system be used sparingly and disabled after the desired information is captured. This is 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.

Reduction in False Positives

The wIPS facilitates a reduction in false positives with respect to security monitoring of the wireless network, and correlates attack signatures. wIPS triggers an alarm whenever it detects a number of management frames over the air that are causing damage to the wireless infrastructure network. This is 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.

Alarm Aggregation

One major difference between the existing Cisco controller-based IDS system and its wIPS system is that 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 is forwarded to the Prime Infrastructure once because alarm aggregation takes place on the Mobility Services Engine. The existing controller-based IDS system does not aggregate alarms. This figure shows the alarm aggregation using Cisco controller-based IDS versus wIPS.

Figure 6: Alarm Aggregation Using Cisco Controller-based IDS Versus wIPS
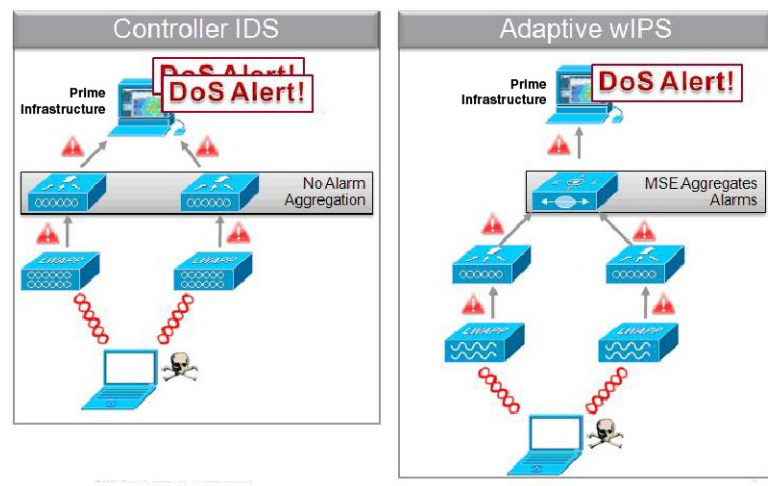
Another major difference between the controller-based IDS and wIPS is the number of attacks that each system can detect. As described in the subsections and shown in the below tables, wIPS can detect a multitude of attacks and attack tools. These attacks include both denial of service (DoS) attacks and security penetration attacks. This section contains the following topics:

User Authentication and Encryption

User authentication and wireless traffic encryption acts as a defense for WLAN security. User authentication blocks out unauthorized access to your wired and wireless resources. Traffic encryption prevents intruders from eavesdropping into the wireless traffic. Common security violations in the authentication and encryption category include misconfiguration, out-of-date software, and suboptimal choice of corporate security policy.

The following table shows the wIPS Security attacks detected by the controller-based IDS and wIPS service.

Table 2: Security Attack Detection by Controller IDS and wIPS

Alarm Name	Detected By Controller IDS	Detected By wIPS
Static WEP encryption		
AP with encryption disabled		X
Client with encryption disabled		X
Crackable WEP IV key used		X
Device using open authentication		X
Device using shared key authentication		X
WEP IV key reused		X
WPA and 802.11i		
802.1x rekey timeout too long		X
802.1x unencrypted broadcast or multicast		X
AP not protected by EAP-TLS		X
Device unprotected by Selected Authentication Methods		X
Device not using EAP -TTLS		X
Device unprotected by 802.11i/AES		X
Device unprotected by 802.1x		X
Device unprotected by EAP-FAST		X
Device unprotected by PEAP		X
Device unprotected by TKIP		X
WPA or 802.11i pre-shared key used		X

DoS Attacks

A DoS attack involves mechanisms that 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 the ability of a wireless network to deliver reliable services, it does not result in a data breach and its negative consequences are often over once the attack has stopped.

The following table compares the DoS attacks detected by the controller-based IDS and wIPS service.

Table 3: DoS Attack Detection by Controller IDS and wIPS

Alarm Name	Detected By Controller IDS	Detected By wIPS
DoS Attack Against AP		
Association flood	X	X
Association table overflow		X
Authentication flood	X	X
EAPOL-Start attack	X	X
PS-Poll flood		X
Probe request flood		X
Re-association request flood		X
Unauthenticated Association		X
DoS Attack Against Infrastructure		
Beacon flood		X
CTS flood		X
MDK3-Destruction attack		X
Queensland University of Technology Exploit		X
RF jamming attack		X
RTS flood		X
Virtual carrier attack	X	X
DoS Attack Against Station		

Alarm Name	Detected By Controller IDS	Detected By wIPS
Authentication-failure attack		X
Block ACK flood		X
De-Auth broadcast flood	X	X
De-Auth flood	X	X
Dis-Assoc broadcast flood		X
Dis-Assoc flood	X	X
EAPOL-Logoff attack	X	X
FATA-Jack tool		X
Premature EAP-Failure		X
Premature EAP-Success		X
Probe response flood		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.

The below table compares the security penetration attacks detected by the controller-based IDS and wIPS service

Table 4: Security Penetration Attack Detection by Controller IDS and wIPS

Alarm Name	Detected by Controller IDS	Detected by wIPS	
ASLEAP tool detected	X	X	
AirDrop Session dected		X	
AirPwn		X	
Airsnarf attack		X	
Bad EAP-TLS frames		X	

Alarm Name	Detected by Controller IDS	Detected by wIPS
Beacon Fuzzed Frame Detected		X
Brute Force Hidden SSID	X	X
ChopChop Attack		X
DHCP Starvation Attack detected		X
Day-Zero attack by WLAN security anomaly	X	X
Day-zero attack by device security anomaly		X
Device Broadcasting XSS SSID		X
Device probing for APs		X
Dictionary attack on EAP methods		X
EAP attack against 802.1x authentication		X
Fake APs detected	X	X
Fake DHCP server detected		X
Fast WEP crack tool detected		X
Fragmentation Attack		X
HT-Intolerant degradation of service		X
Honeypot AP detected	X	X
Hotspotter tool detected		X
Identical send and receive address		X
Improper broadcast frames		X

Alarm Name	Detected by Controller IDS	Detected by wIPS
Karma tool detected		X
Malformed 802.11 packets detected		X
Man in the middle attack detected		X
NetStumbler detected	X	X
Netstumbler victim detected	X	X
PSPF violation detected		X
Probe Request Fuzzed Frame Detected		X
Probe Response Fuzzed Frame Detected		X
Soft AP or Host AP detected		X
Spoofed MAC address detected		X
Suspicious after-hours traffic detected		X
Unauthorized association by vendor list		X
Unauthorized association detected		X
Wellenreiter detected	X	X
WiFi Protected Setup Pin brute force		X
WiFiTap tool detected		X
Channel or Device Overload		
AP Association Capacity full		X
AP overloaded by stations		X

Alarm Name	Detected by Controller IDS	Detected by wIPS
AP overloaded by utilization		X
Excessive Bandwidth usage		X
Excessive multicast/broadcast on channel		X
Excessive multicast/broadcast on node		X

wIPS Alarm Flow

The wIPS system follows a linear chain of communication to propagate attack information obtained from initially scanning the airwaves to forwarding information to the Prime Infrastructure. This figure shows the alarm flow within the wireless network.

Figure 7: Alarm Flow Within Network
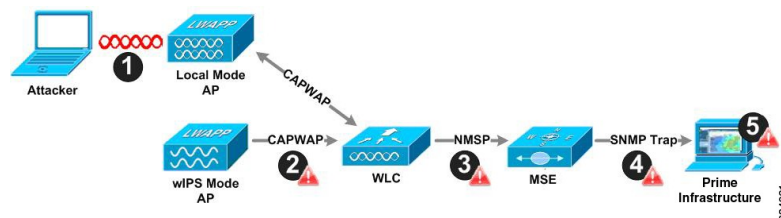
1 For an alarm to be triggered on the wIPS system, an attack must be launched against a legitimate access point or client. Legitimate access points and clients are discovered automatically in a CUWN by trusting devices broadcasting the same RF Group name. In this configuration, the system dynamically 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 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 the Prime Infrastructure. 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 the Prime Infrastructure.

5 The SNMP trap containing the alarm information is received and displayed by the Prime Infrastructure.

Performance Violation

WLAN performance efficiency is challenged by the dynamics of the RF environment and the mobility of the client devices. WLAN performance and efficiency is ensured by the wIPS by monitoring the WLAN and alerting the wireless administrator on early warning signs for trouble. To maximize the use of wIPS, performance alarms can be customized to match the WLAN deployment specification.

The following table shows the Performance Violation detected by the controller-based IDS and wIPS service.

Table 5: Performance Violation Detection by Controller IDS and wIPS

Alarm Name	Detected By Controller IDS	Detected By wIPS
Channel or Device Overload		
AP association capacity full		X
AP overloaded by stations		X
AP overloaded by utilization		X
Excessive Bandwidth usage		X
Excessive multicast/broadcast on channel		X
Excessive multicast/broadcast on node		X

Forensics

The Cisco wIPS system provides the ability to capture forensic attacks 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 the Prime Infrastructure.

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 through CAPWAP, which then forwards the forensic file through 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 the Prime Infrastructure 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 that supports this format. Wireshark is available at http://www.wireshark.org

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 the Prime Infrastructure 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 percent, an anomaly alarm is triggered on the Mobility Services Engine. This alarm is then sent to the Prime Infrastructure to inform the administrator that something else is happening in the wireless network beyond traditional attacks that the system may encounter. The anomaly detection alarm can also be employed to detect day zero attacks that might not have a pre-existing 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.

Auto MAC Learning Of Valid Clients

The Auto MAC learning feature is introduced in Release 7.5. This feature protects valid clients on your network from connecting to rogue APs. The MSE is used to validate the clients without any pre-configuration on the MSE.

Whenever a client is connecting to Rogue AP, the controller validates whether the client is valid or not with the MSE. If the client is valid, then controller auto contains the client from connecting to the rogue AP. Controller uses the MSE auto MAC learning database to check each re-association request MAC address.

Note   You need to enable the Auto MAC learning of valid clients feature from the Cisco Controller UI.

Figure 8: Auto MAC Learning of Valid Clients
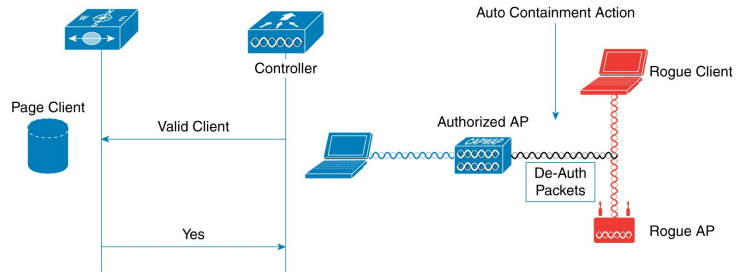
C H A P T E R **2**

Adding and Deleting Mobility Services Engines and Licenses

This chapter describes how to add and delete a Cisco 3300 series Mobility Services Engine (MSE) to and from the Cisco Prime Infrastructure.

Note   The MSEs, Synchronize Services, Synchronization History, High Availability, Context Aware Notifications, and Mobile Concierge pages on the Identity Services tab are available only in the root virtual domain in Release 7.3.101.0.

Licensing Requirements for MSE

See Cisco Mobility Services Ordering and Licensing Guide for MSE license information.

MSE License Structure Matrix

The following table lists the breakup of licenses between the high-end, low-end, and evaluation licenses for the MSE, Location services or Context-Aware Service software, and wIPS.

Table 6: MSE License Structure Matrix

	High End	**Low End**	**Evaluation**
MSE Platform	High-end appliance and infrastructure platform.	Low-end appliance and infrastructure platform.	120 days.
Location Service or Context-Aware Service software	3000, 6000, 12,000 access points	1000 access points	120 days, 100 tags and 100 elements.
	3000, 6000, 12,000 access points	1000 elements	
wIPS	6000 access points	2000 access points	120 days, 20 access points.

Note   Contact Cisco account representative to extend evaluation licenses if required.

Sample MSE License File

The following is a sample MSE license file:

```
Feature MSE Cisco 1.0 permanent uncounted \

VENDOR_STRING=UDI=udi,COUNT=1 \

HOSTID=ANY \

NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</Li cLineID> \
<PAK>dummyPak</PAK>" \

SIGN="0C04 1EBA BE34 F208 404F 98ED 43EC \

45D7 F881 08F6 7FA5 4DED 43BC AF5C C359 0444 36B2 45CF 6EA6 \

1DB1 899F 413F F543 F426 B055 4C7A D95D 2139 191F 04DE"
```

This sample file has five license entries. First word in the first line of any license entry will tell you what type of license it is. It can either be a Feature or Increment license. A Feature license is static, lone-item license. An Increment license is an additive license. In the MSE, each service engine is treated as Increment licenses.

The second word in the first line defines the specific component to be licensed (for example, MSE). The third word defines the vendor of the license (for example, Cisco). The fourth word defines the version of the license (for example, 1.0). The fifth word defines the expiration date; this can be permanent for licenses that never expire or a date in the format dd-mmm-yyyy. The last word defines whether this license is counted.

Revoking and Reusing an MSE License

You can revoke an MSE appliance license from one system and reuse it on another system. When you revoke a license, the license file is deleted from the system. If you want to reuse the license on another system, then the license needs to be rehosted.

If you want to reuse a license with an upgrade SKU on another system, then you need to have the corresponding base license SKU installed in the system to which you want to reuse the upgrade SKU. You cannot reuse the upgrade license SKU in a system if the corresponding base license SKU is deleted from it.

When you revoke a license, the MSE restarts the individual service engines to reflect the changes to the licenses. Then the service engines receives the updated capacity from MSE during startup.

For more information on licensing, see the *Cisco Prime Infrastructure Configuration Guide*, *Release 1.4*.

Guidelines and Limitations

Follow these guidelines when adding an MSE to the Prime Infrastructure and registering device and wIPS product authorization keys:

- From release 7.5 onwards, wIPS service requires a separate MSE.

- After adding a new MSE, you can synchronize network designs (campus, building, and outdoor maps), Cisco WLC, switches (Catalyst 3000 series and 4000 series only), and event groups for the Mobility Services Engine and the Prime Infrastructure.

> **Note** From Release 7.5 onwards, Cisco Engine for Clients and Tags is used to track tags. If a tag license is detected when you are upgrading from Release 7.2 and later Releases to Release 7.5, then a warning message is displayed about removing the AeroScout license and engine. If you accept, then it removes all the partner engine sub services and Cisco Tag Engine sub service is enabled by default. If you do not accept the removal of partner engine, then it continues with the installation. While upgrading, if no tag licenses are detected, then the installation proceeds as before.

- If you had changed the username and password during the automatic installation script, enter those values here while adding a MSE to the Prime Infrastructure. If you did not change the default passwords, we recommend that you rerun the automatic installation script and change the username and password.

Adding a Mobility Services Engine to the Prime Infrastructure

You can add MSE using the Add Mobility Services Engine dialog box in the Mobility Service page. In this dialog box, you can add licensing files, tracking parameters, and assign maps to MSE. If you launch the wizard with an existing MSE for configuration, then the Add MSE option appears as Edit MSE Details.

Cisco Wireless Intrusion Prevention System Configuration Guide, Release 8.0

Tip To learn more about Cisco Adaptive wIPS features and functionality, go to http://www.cisco.com/ to watch a multimedia presentation. Here you can find the learning modules for a variety of the Prime Infrastructure topics. Over future releases, there will be more overview and technical presentations to enhance your learning.

Note The Prime Infrastructure Release 1.0 recognizes and supports MSE 3355 appropriately.

Note The **Services** > **Mobility Services Engine** page is available only in the virtual domain in Release 7.3.101.0.

To add a Mobility Services Engine to the Prime Infrastructure, log in to the Prime Infrastructure and follow these steps:

Step 1 Verify that you can ping the Mobility Services Engine.

Step 2 Choose **Services** > **Mobility Services Engines** to display the Mobility Services page.

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

Step 4 In the **Device Name** text box, enter a name for the MSE.

Step 5 In the **IP Address** text box, enter the IP address of the MSE.

Step 6 (Optional) In the **Contact Name** text box, enter the name of the MSE administrator.

Step 7 In the **User Name** and **Password** text boxes, enter the username and password for the MSE.
This refers to the Prime Infrastructure communication username and password created during the setup process.

If you have not specified the username and password during the setup process, use the defaults.

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, we recommend that you rerun the automatic installation script and change the username and password.

Step 8 Select the **HTTPS** check box to allow communication between the MSE and third-party applications. By default, the Prime Infrastructure uses HTTPSs to communicate with the MSE.

Step 9 Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the MSE.
This option is applicable for network designs, wired switches, Cisco WLCs, and event definitions. The existing location history data is retained, however, you must use manual service assignments to perform any future location calculations.

Step 10 Click **Next**. The Prime Infrastructure automatically synchronizes the selected elements with the MSE.
After the synchronization, the MSE License Summary page appears. You can use the MSE License Summary page to install a license, add a license, remove a license, install an activation license, and install service license. The Select Mobility Service page appears.

Step 11 To enable a service on the Mobility Services Engine, select the check box next to the service. Services include Context-Aware Service and wIPS.
You can choose CAS to track clients, rogues, interferers, wired clients, and tags.

Choose Cisco Tag Engine to track tags.

Step 12   Click **Save**.

Note   After adding a new MSE, you can synchronize network designs (campus, building, and outdoor maps), Cisco WLCs, switches (Catalyst Series 3000 only), and event groups on the local MSE using the Prime Infrastructure. You can perform this synchronization immediately after adding a new MSE or at a later time. To synchronize the local and the Prime Infrastructure databases, see Synchronizing Mobility Services Engines, on page 29.

Enabling Services on the Mobility Services Engine

To enable services on the Mobility Services Engine, follow these steps:

Step 1   After adding the license file, the Select Mobility Service page appears.

Step 2   To enable a service on the MSE, select the check box next to the service. The different type of services are as follows:

- Context Aware Service—If you select the Context Aware Service check box, then you must select a location engine to perform location calculation. You can choose **CAS to track clients**, **rogues**, **interferers**, and **tags**. You can choose Cisco Context-Aware Engine for Clients and Tag to track tags.

- Wireless Intrusion Prevention System—If you select the Wireless Intrusion Prevention System check box, it detects wireless and performance threats.

- Mobile Concierge Service—If you select the Mobile Concierge Service check box, it provides service advertisements that describe the available services for the mobile devices.

- CMX Analytics Service—If you select the CMX Analytics Service check box, it provides a set of data analytic tools packaged for analyzing Wi-Fi device location data that comes from the MSE.

Note   From release 7.5 onward, wIPS service requires a dedicated MSE because it does not support CAS and wIPS on the same MSE.

Step 3   Click **Next** to configure the tracking parameters.

Step 4   After you enable services on the MSE, the Select Tracking & History Parameters page appears.

Note   If you skip configuring the tracking parameters, the default values are selected.

Step 5   You can select the clients that you want to keep track of by selecting the corresponding Tracking check box(es). The various tracking parameters are as follows:

- Wired Clients

- Wireless Clients

- Rogue Access Points

    ◦ Exclude Adhoc Rogue APs

- Rogue Clients

- Interferers

- Active RFID Tags

Step 6   You can enable the history tracking of devices by selecting the corresponding devices check box(es). The different history parameters are as follows:

- Wired Stations

- Client Stations

- Rogue Access Points

- Rogue Clients

- Interferers

- Asset Tags

Note   If the history tracking is not enabled, the MSE CAS service will not store historical data.

Step 7   Click **Next** to Assign Maps to the MSE.

Note   The Assigning Maps page is available only if you select CAS as one of the services to be enabled on the MSE.

Step 8   Once you configure MSE tracking and history parameters, the Assigning Maps page appears.
The Assign Maps page shows the following information:

- Map Name

- Type (building, floor, campus)

- Status

Step 9   You can see the required map type by selecting All, Campus, Building, Floor Area, or Outdoor Area from the Filter option available in the page.

Step 10   To synchronize a map, select the **Name** check box, and click **Synchronize**.
Upon synchronization of the network designs, the appropriate Cisco WLCs that have APs assigned on a particular network design are synchronized with the MSE automatically. Click **Done** to save the MSE settings.

Configuring MSE Tracking and History Parameters

Step 1   After you enable services on the Mobility Services Engine, the Select Tracking & History Parameters page appears.

Note   If you skip configuring the tracking parameters, the default values are selected.

Step 2   You can select the clients that you want to keep track of by selecting the corresponding Tracking check box(es). The various tracking parameters are as follows:

- Wired Clients

- Wireless Clients

- Rogue Access Points

  ◦ Exclude Adhoc Rogue APs

- Rogue Clients

- Interferers

- Active RFID Tags

Step 3 You can enable the history tracking of devices by selecting the corresponding devices check box(es). The different history parameters are as follows:

- Wired Stations

- Client Stations

- Rogue Access Points

- Rogue Clients

- Interferers

- Asset Tags

Step 4 Click **Next** to Assign Maps to the MSE.

Assigning Maps to the MSE

Note The Assigning Maps page is available only if you select CAS as one of the services to be enabled on the MSE.

To assign maps to the MSE, follow these steps:

Step 1 Once you configure MSE tracking and history parameters, the Assigning Maps page appears.
The Assign Maps page shows the following information:

- Map Name

- Type (building, floor, campus)

- Status

Step 2 You can see the required map type by selecting All, Campus, Building, Floor Area, or Outdoor Area from the Filter option available on the page.

Step 3 To synchronize a map, select the **Name** check box, and click **Synchronize**.
Upon synchronization of the network designs, the appropriate Cisco WLCs that have APs assigned on a particular network design are synchronized with the MSE automatically. Click **Done** to save the MSE settings.

Deleting an MSE License File

To delete an MSE license file, follow these steps:

Step 1   Choose **Services** > **Mobility Service Engine**.
The Mobility Services page appears.

Step 2   Select the Mobility Services Engine(s) to be deleted by selecting the corresponding **Device Name** check box(es).

Step 3   From the Select a command drop-down list, choose **Edit Configuration**.
The Edit Mobility Services Engine dialog box appears.

Step 4   Click **Next** in the Edit Mobility Services Engine dialog box.
The MSE License Summary page appears.

Step 5   Choose the MSE license file that you want to delete in the MSE License Summary page.

Step 6   Click **Remove License**.

Step 7   Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the license.

Deleting a Mobility Services Engine from the Prime Infrastructure

To delete one or more Mobility Services Engines from the Prime Infrastructure database, follow these steps:

Step 1   Choose **Services > Mobility Services Engines**.
The Mobility Services page appears.

Step 2   Select the MSE to be deleted by selecting the corresponding **Device Name** check box(es).

Step 3   From the Select a command drop-down list, choose **Delete Service(s)**. Click **Go**.

Step 4   Click **OK** to confirm that you want to delete the selected MSE from the Prime Infrastructure database.

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

Registering Device and wIPS Product Authorization Keys

You receive a Product Authorization Key (PAK) when you order a CAS element, wIPS, or tag license from Cisco. You must register the PAK to receive the license file for installation on the Mobility Services Engine. License files are e-mailed to you after successfully registering a PAK. Client and wIPS PAKs are registered with Cisco.

To register a PAK to obtain a license file for installation, follow these steps:

Step 1   On your web browser, go to http://tools.cisco.com/SWIFT/LicensingUI/Home.

Step 2   Enter the PAK, and click **SUBMIT**.

Step 3   Verify the license purchase. Click **Continue** if correct . The licensee entry page appears.

            Note   If the license is incorrect, click the **TAC Service Request Tool** URL to report the problem.

Step 4   In the Designate Licensee page, enter the UDI of the MSE in the Host Id text box. This is the Mobility Services Engine on which the license is installed.

            Note   UDI information for a Mobility Services Engine is found in the General Properties at **Services** > **Mobility Services Engine** > *Device Name* > *System*.

Step 5   Select the **Agreement** check box. Registrant information appears beneath the Agreement check box.

Step 6   If the registrant and end user are not the same person, select the **Licensee (End-User)** check box beneath registrant information and enter the information for the end user.

Step 7   Click **Continue**. A summary of entered data appears.

Step 8   In the Finish and Submit page, review registrant and end-user data. Click **Edit Details** to correct any information. Click **Submit**. A confirmation page appears.

Installing Device and wIPS License Files

You can install device and wIPS licenses from the Prime Infrastructure. From Release 7.5 onwards, Cisco Engine for Clients and Tags is used to track tags. If a tag license is detected when you are upgrading from Release 7.2 and later releases to Release 7.5, then a warning message is displayed about removing the AeroScout license and engine. If you accept, then it removes all the partner engine sub services and Cisco Tag Engine sub service is enabled by default. If you do not accept to remove the partner engine, then it will continue with the installation. If there are no tag licenses are detected, then the installation will proceed as before.

The Administration > License Center page is available only in the virtual domain in Release 7.3.101.0 and later.

To add a device or wIPS license to the Prime Infrastructure after registering the PAK, follow these steps:

Step 1   Choose **Administration > Licenses**.

Step 2   Choose **Files** > **MSE Files** from the left sidebar menu.

Step 3   Click **Add**. The Add a License File dialog box appears.

Step 4   Choose the applicable MSE name from the **MSE Name** drop-down list.

            Note   Verify that the UDI of the selected Mobility Services Engine matches the one that you entered when registering the PAK.

Step 5   Click **Browse** to select the license file.

Step 6   Click **Ok**. The newly added license appears in the MSE license file list.

C H A P T E R 3

Synchronizing Mobility Services Engines

This chapter describes how to synchronize Cisco WLCs and the Prime Infrastructure with Cisco Mobility Services Engines.

> **Note** The Mobility Services Engines, Synchronize Services, Synchronization History, High Availability, Context Aware Notifications, and MSAP pages on the Services tab are available in Release 7.3.101.0.

Synchronizing the Prime Infrastructure and Mobility Services Engines

This section describes how to synchronize the Prime Infrastructure and Mobility Services Engines manually and automatically.

> **Note** The Services > Synchronize Services page is available only in the virtual domain in Release 7.3.101.0 and later.

After adding a MSE to the Prime Infrastructure, you can synchronize network designs (campus, building, floor, and outdoor maps), controllers (name and IP address), specific Catalyst 3000 series and 4000 series switches, and event groups with the MSE.

- Network Design—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.

- Cisco WLC—A selected Cisco WLC that is associated and regularly exchanges location information with a MSE. Regular synchronization ensures location accuracy.

- Wired Switches—Wired Catalyst switches that provide an interface to wired clients on the network. Regular synchronization ensures that location tracking of wired clients in the network is accurate.

  ◦ The MSE 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 MSE can also be synchronized with the following Catalyst 4000 series switches: 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—A group of predefined events that define triggers that generate an event. Regular synchronization ensures that the latest defined events are tracked. Event groups can also be created by third-party applications. For more information on third-party application created event groups, see the Configuring Automatic Database Synchronization and Out-of-Sync Alerts, on page 33.

- Third Party Elements—When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.

- Service Advertisements—Mobile Conceirge Service provides service advertisements on mobile devices. This shows the service advertisement that is synchronized with the MSE.

Prerequisites for Synchronizing Mobility Services Engine

- Be sure to verify software compatibility between the Cisco WLC, Prime Infrastructure, and the Mobility Services Engine before synchronizing. See the latest Mobility Services Engine release notes at the following URL: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

- Communication between the MSE, Prime Infrastructure, and the Cisco WLC is in Coordinated Universal Time (UTC). Configuring NTP on each system provides devices with UTC time. The MSE and its associated controllers must be mapped to the same NTP server and the same Prime Infrastructure server. An NTP server is required to automatically synchronize time between the controller, Prime Infrastructure, and the MSE. However, the timezone for MSE and controller should still be set to UTC. This is because wIPS alarms require MSE and controller time to be set to UTC.

Working with Third-Party Elements

When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.

Deleting the Elements or Marking Them as Third-Party Elements

To delete the elements or mark them as third-party elements, follow these steps:

Step 1 Choose **Services** > **Synchronize Services**.
The Network Designs page appears.

Step 2 In the Network Designs page, choose **Third Party Elements** from the left sidebar menu.
The Third Party Elements page appears.

Step 3 Select one or more elements.

Step 4 Click one of the following buttons:

- **Delete Event Groups**—Deletes the selected event groups.

- **Mark as 3rd Party Event Group(s)**—Marks the selected event groups as third-party event groups.

Synchronizing Cisco WLC with a Mobility Services Engine

This section describes how to synchronize a Cisco WLCs, assign an MSE to any Cisco WLCs and also to unassign a network design, Cisco WLCs, wired switch, or event group from a Mobility Services Engine.

Assigning and Synchronizing Network Designs, a Cisco WLC, Catalyst Switch, or Event Group

To synchronize network designs, a Cisco WLC, a Catalyst switch, or event group with the Mobility Services Engine, follow these steps:

Step 1 Choose **Services** > **Synchronize Services**.
The left sidebar menu contains the following options: **Network Designs**, **Controllers**, **Event Groups**, **Wired Switches**, **Third Party Elements**, and **Service Advertisements**.

Step 2 From the left sidebar menu, choose the appropriate menu options.

Step 3 To assign a network design to a MSE, in the Synchronize Services page, choose **Network Designs** from the left sidebar menu.
The Network Designs page appears.

Step 4 Select all the maps to be synchronized with the MSE by selecting the corresponding **Name** check box.

> **Note** Through Release 6.0, you can assign only up to a campus level to a MSE. Starting with Release 7.0, this option is granular to a floor level. For example, you can choose to assign floor1 to MSE 1, floor2 to MSE 2, and floor3 to MSE 3.

Step 5 Click **Change MSE Assignment**.

Step 6 Select the MSE to which the maps are to be synchronized.

Step 7 Click either of the following in the MSE Assignment dialog box:

- **Synchronize**—Synchronizes the MSE assignment.

- **Cancel**—Discards the changes to MSE assignment and returns to the Network Designs page.

  You can also click **Reset** to undo the MSE assignments.

> **Note** A network design may include a floor in a campus or a large campus with several buildings, each monitored by a different MSE. Because of this, you may need to assign a single network design to multiple MSEs. The network design assignments also automatically pick up the corresponding Cisco WLC for synchronization.

Step 8 Click **Synchronize** to update the MSE(s) database(s).

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

You can use the same procedure to assign wired switches or event groups to a MSE. To assign a Cisco WLC to a MSE, see the Synchronizing Controllers with a Mobility Services Engine, page 3-3 for more information.

> **Note** It is important to have a clock sync between the WLC and MSE to ensure proper synchronization. If synchronization fails, check if the two devices share the same NTP clock source.

Assigning an MSE to the Cisco WLC

To assign a Mobility Services Engine with any Cisco WLC on a per-service basis (CAS or wIPS), follow these steps:

Step 1 Choose **Services** > **Synchronize Services**.

Step 2 In the Network Designs page, choose **Controller** from the left sidebar menu.

Step 3 Select the Cisco WLCs to be assigned to the Mobility Services Engine by selecting the corresponding **Name** check box.

Step 4 Click **Change MSE Assignment**.

Step 5 Choose MSEs dialogue box appears. You can choose **CAS**, **wIPS** or **MSAP** option.

Step 6 Choose the MSE to which the Cisco WLCs must be synchronized.

Step 7 Click either one of the following in the Choose MSEs dialog box:

- **Synchronize**—Synchronizes the MSE assignment.

- **Cancel**—Discards the changes to MSE assignment and returns to the **Controllers** page.

  You can also click **Reset** to undo the MSE assignments.

Step 8   Click **Synchronize** to complete the synchronization process.

Step 9   Verify that the MSE is communicating with each of the Cisco WLCs for only the chosen service. This can be done by clicking the NMSP status link in the status page.

    Note   After synchronizing a Cisco WLC, verify that the timezone is set on the associated Cisco WLC.

    Note   Controller names must be unique for synchronizing with a MSE. If you have two Cisco WLCs with the same name, only one is synchronized. You can use the same procedure to assign Catalyst switches or event groups to a MSE.

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

Unassigning a Network Design, Wired Switch, or Event Group from MSE

To unassign a network design, controller, wired switch, or event group from a Mobility Services Engine, follow these steps:

Step 1   Choose **Services** > **Synchronize Services**.

Step 2   From the left sidebar menu, choose the appropriate menu options.

Step 3   Select one or more elements by selecting the **Name** check box, and click **Change MSE Assignment**.
The Choose MSEs dialog box appears.

Step 4   On the respective tabs, choose one or more elements, and click **Change MSE Assignment**.

Step 5   Unselect the MSE if you do not want the elements to be associated with that MSE by selecting either the **CAS** or **MSAP** check box.

Step 6   Click **Synchronize**.
The Sync Status column appears blank.

Step 7   Click **Cancel** to discard the changes to MSE assignment and to return to the Controllers page.

Configuring Automatic Database Synchronization and Out-of-Sync Alerts

Manual synchronization of the Prime Infrastructure and Mobility Services Engine databases is immediate. However, future deployment changes (such as changes to maps and access point positions) can yield incorrect location calculations and asset tracking until resynchronization.

To prevent out-of-sync conditions, use the Prime Infrastructure to carry out synchronization. This policy ensures that synchronization between the Prime Infrastructure and MSE databases is triggered periodically and any related alarms are cleared.

Any change made to one or more of any synchronized component is automatically synchronized with the MSE. For example, if a floor with access points is synchronized with a particular MSE and then one access point is moved to a new location on the same floor or another floor that is also synchronized with the MSE, then the changed location of the access point is automatically communicated.

Cisco Wireless Intrusion Prevention System Configuration Guide, Release 8.0

To further ensure that the Prime Infrastructure and MSE are in sync, smart synchronization happens in the background.

- Configuring Automatic Database Synchronization, on page 34
- Smart Controller Assignment and Selection Scenarios, on page 34
- Out-of-Sync Alarms, on page 35

Configuring Automatic Database Synchronization

To configure smart synchronization, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the **Mobility Service Synchronization** check box and click the **Mobility Service Synchronization** link.
The Mobility Services Synchronization page appears.

Step 3 To set the Mobility Services Engine to send out-of-sync alerts, select the Out of Sync Alerts **Enabled** check box.

Step 4 To enable smart synchronization, select the Smart Synchronization **Enabled** check box.
   Note Smart synchronization does not apply to elements (network designs, controllers, or event groups) that have not yet been assigned to a MSE. However, out-of-sync alarms are still generated for these unassigned elements. For smart synchronization to apply to these elements, you must manually assign them to a MSE.
   Note When a MSE is added to a Prime Infrastructure, the data in the Prime Infrastructure is always treated as the primary copy that is synchronized with the MSE. All synchronized network designs, controllers, event groups, and wired switches that are present in the MSE and not in the Prime Infrastructure are removed automatically from MSE.

Step 5 Enter the time interval, in minutes, that the smart synchronization is to be performed.
By default, the smart-sync is enabled.

Step 6 Click **Save**.
For Smart controller assignment and selection scenarios, see the Smart Controller Assignment and Selection Scenarios, on page 34.

Smart Controller Assignment and Selection Scenarios

Scenario 1

If a floor having at least one access point from a controller is chosen to be synchronized with the Mobility Services Engine in the Network Designs menu of the Synchronize Services page, then the controller to which that access point is connected is automatically selected to be assigned to the Mobility Services Engine for CAS service.

Scenario 2

When at least one access point from a controller is placed on a floor that is synchronized with the Mobility Services Engine, the controller to which the access point is connected is automatically assigned to the same MSE for the CAS service.

Scenario 3

An access point is added to a floor and assigned to a MSE. If that access point is moved from controller A to controller B, then controller B is automatically synchronized to the MSE.

Scenario 4

If all access points placed on a floor that is synchronized to the MSE are deleted, then that controller is automatically removed from the MSE assignment or unsynchronized.

Out-of-Sync Alarms

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

- Elements are modified in the Prime Infrastructure (the auto-sync policy pushes these elements).

- Elements other than Cisco WLCs exist in the Mobility Services Engine database but not in the Prime Infrastructure.

- Elements are not assigned to any MSE (the auto-sync policy does not apply).

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

- The MSE is deleted

> **Note** When you delete a MSE, the out-of-sync alarms for that system are also deleted. In addition, if you delete the last available MSE, the alarm for the following event: "elements not assigned to any server" is 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 the Status of Mobility Services Engine Synchronization

You can use the Synchronize Services feature in the Prime Infrastructure to view the status of network design, controller, switch, and event group synchronization with a Mobility Services Engine.

Viewing the Status of Mobility Services Engine Synchronization

To view the synchronization status, follow these steps:

Step 1 Choose **Services > Synchronize Services**.

Step 2 From the left sidebar menu, choose **Network Designs**, **Controllers**, **Wired Switches**, **Third Party Elements**, or **Service Advertisements**.

For each of the elements, the Sync. Status column shows the synchronization status. A green two-arrow icon indicates that its corresponding element is synchronized with the specified server such as a Mobility Services Engine. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a provided server.

The Message column shows the reason for failure if the elements are out of sync.

You can also view the synchronization status at **Monitor** > **Maps** > **System Campus** > *Building* > *Floor*.

where *Building* is the building within the campus and *Floor* is a specific floor in that campus building.

The MSE Assignment option on the left sidebar menu shows which Mobility Services Engine the floor is currently assigned to. You can also change the Mobility Services Engine assignment in this page.

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, choose **Services** > **Synchronization History**. The Synchronization History page appears. The following table lists the Synchronization History Page parameters.

Table 7: Synchronization History Page

Text Boxes	Description
Timestamp	The date and time at which the synchronization has happened.
Server	The Mobility Services Engine server.
Element Name	The name of the element that was synchronized.
Type	The type of the element that was synchronized.
Sync Operation	The sync operation that was performed. It can either be an Update, Add, or Delete.
Generated By	The method of synchronization. It can either be Manual or Automatic.
Status	The status of the synchronization. It can be either Success or Failed.
Message	Any additional message about the synchronization.

C H A P T E R **4**

Configuring and Viewing System Properties

This chapter describes how to configure and view system properties on the Cisco Mobility Services Engine.

Licensing Requirement

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. They are provided with a 120 day license (time is decremented by the number of days you use it rather than by the number of calendar days passed).

For more information on purchasing and installing licenses, see the following URL:

http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

Editing General Properties and Viewing Performance

General Properties—You can use the Cisco Prime Infrastructure to edit the general properties of a Mobility Services Engine such as contact name, username, password, services enabled on the system, enabling or disabling a service, or enabling the MSE for synchronization. See the Editing General Properties, on page 38 for more information.

Note   Use the general properties to modify the username and password that you defined during initial setup of the MSE.

Performance—You can use the Prime Infrastructure to view CPU and memory usage for a given MSE. See the Viewing Performance Information, on page 40 for more information.

This section contains the following topics:

Editing General Properties

To edit the general properties of a Mobility Services Engine, follow these steps:

Step 1 Choose **Services** > **Mobility Services Engines** to display the Mobility Services page.

Step 2 Click the name of the MSE you want to edit. Two tabs appear with the following headings: General and Performance.

Note If the General Properties page is not displayed by default, choose **Systems** > **General Properties** from the left sidebar menu.

Step 3 Modify the fields as appropriate on the General tab. This table lists the General Properties page fields.

Table 8: General Tab

Field	Configuration Options
Device Name	User-assigned name for the MSE.
Device Type	Indicates the type of MSE (for example, Cisco 3310 MSE). Indicates whether the device is a virtual appliance or not.
Device UDI	The Device UDI (Unique Device Identifier) is the string between double quote characters (including spaces in the end if any).
Version	Version of product identifier.
Start Time	Indicates the start time when the server was started.
IP Address	Indicates the IP address for the MSE.
Contact Name	Enter a contact name for the MSE.
User Name	Enter the login username for the Prime Infrastructure server that manages the MSE. This replaces any previously defined username including any set during initial setup.
Password	Enter the login password for the Prime Infrastructure server that manages the MSE. This replaces any previously defined password including any set during initial setup.
Legacy Port	Enter the mobility services port number that supports HTTPS communication. The Legacy HTTPS option must also be enabled.
Legacy HTTPS	This does not apply to MSEs. It applies only to location appliances.

Field	Configuration Options
Delete synchronized service assignments and enable synchronization	Select this check box if you want to permanently remove all service assignments from the MSE. This option shows up only if the delete synchronized service assignments check box was unselected while adding a MSE.
Mobility Services	To enable a service on the MSE, select the check box next to the service. The services include Context Aware, wIPS, Mobile Concierge, CMX Analytics, CMX Browser Engage, and Proxy service. You can choose CAS to track clients, rogues, interferers, wired clients, and tags. Choose either of the following engines to track tags: • Cisco Tag Engine or • Partner Tag Engine **Note** The Partner Tag Engine is used only to track the tags. The clients are still tracked by Cisco Context-Aware Engine. **Note** Once selected, the service is displayed as Up (active). All inactive services are noted as Down (inactive) on the selected (current) system and on the network. **Note** From release 7.5 onward, wIPS service requires a dedicated MSE because it does not support CAS and wIPS on the same MSE. Click the **here** link to see the number of devices that can be assigned for the current system. In the License Center page, choose **MSE** from the left sidebar menu option to see the license details for all MSEs on the network. **Note** For more information on purchasing and installing licenses, see the following URL: 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 the MSE in Release 6.0: tcp 22: MSE SSH port, tcp 80: MSE HTTP port, tcp 443: MSE HTTPS port, tcp 1411: , tcp 8001: Legacy port. Used for location APIs.

Note The following udp ports are in use on the MSE in Release 6.0: udp 123: NTPD port (open after NTP configuration), udp 32768: Location internal port.

Note Port 80 is enabled on the MSE if the **enable http** command was entered on the MSE. Ports 8880 and 8843 are closed on the MSE when the CA-issued certificates are installed on the MSE.

Step 4 Click **Save** to update the Prime Infrastructure and MSE databases.

Viewing Performance Information

To view performance details, follow these steps:

Step 1   Choose **Services > Mobility Services Engines** to display the Mobility Services page.

Step 2   Click the name of the Mobility Services Engine you want to view. Two tabs appear with the following headings: General and Performance.

Step 3   Click the **Performance** tab.
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 page, click the icon at the lower right.

Modifying NMSP Parameters

Network Mobility Services Protocol (NMSP) is the protocol that manages communication between the Mobility Services Engine and the Cisco WLC. Transport of telemetry, emergency, and chokepoint information between the Mobility Services Engine and the Cisco WLC is managed by this protocol.

This menu option is only available in MSE Release 7.0.105.0 and earlier.

- We recommend no change in the default parameter values unless the network is expecting slow response or excessive latency.

- Telemetry, emergency, and chokepoint information is only seen on controllers and the Prime Infrastructure installed with software Release 4.1 and later.

- The TCP port (16113) that the controller and MSE communicate over must be open (not blocked) on any firewall that exists between the controller and MSE for NMSP to function.

To configure NMSP parameters, follow these steps:

Step 1   Choose **Services > Mobility Services Engines**.

Step 2   Click the name of the MSE whose properties you want to edit.

Step 3   Choose **System** > **NMSP Parameters**. The configuration options appear.

Step 4   Modify the NMSP parameters as appropriate. The following table lists the NMSP parameters.

Table 9: NMSP Parameters

Field	Description
IP Address	IP address of the controller or IOS 3E switch.
Target Type	Type of the controller: Controller or IOS 3E switch.

Field	Description
Version	Version of the target device.
NMSP Status	NMSP connection status between MSE and target type.
Echo Request Count	Number of echo request made.
Echo Response Count	Number of echo requests received.
Last Message Received	Timestamp when the last message was received.

Step 5 Click **Save** to update the Prime Infrastructure and MSE databases.

Viewing Active Sessions on a System

You can view active user sessions on the Mobility Services Engine.

To view active user sessions, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the MSE to view its active sessions.

Step 3 Choose **System > Active Sessions**.
For every session, the Prime Infrastructure shows the following information:

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

Adding and Deleting Trap Destinations

You can specify which Prime Infrastructure 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 Prime Infrastructure, that Prime Infrastructure platform automatically establishes itself as the default trap destination. If a redundant Prime Infrastructure configuration exists, the backup Prime Infrastructure is not listed as the default trap destination unless the primary Prime Infrastructure fails and the backup system takes over. Only an active Prime Infrastructure is listed as a trap destination.

Adding Trap Destinations

To add a trap destination, follow these steps:

Step 1 Choose **Services > Mobility Services Engines**.

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 From the Select a command drop-down list, choose **Add Trap Destination**. Click **Go**.
The New Trap Destination page appears.

The following table lists the Add Trap Destination page fields.

Table 10: Add Trap Destination Page Fields

Field	Description
IP Address	IP address for the trap destination.
Port Number	The port number for the trap destination. The default port number is 162.
Destination Type	This field is not editable and has a value of **Other**.
SNMP Version	Choose either **v2c** or **v3** from the SNMP Version drop-down list.
The following set of fields appear only if you select v3 as the SNMP version.	
User Name	The username for the SNMP Version 3.
Security Name	The security name for the SNMP Version 3.
Authentication Type	Choose one of the following from the drop-down list: **HMAC-MD5** **HMAC-SHA**
Authentication Password	The authentication password for the SNMP Version 3.

Field	Description
Privacy Type	Choose one of the following from the drop-down list: **CBC-DES** **CFB-AES-128** **CFB-AES-192** **CFB-AES-256**
Privacy Password	The privacy password for the SNMP Version 3.

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

Step 5   Click **Save**.
You are returned to the Trap Destination Summary page and the newly defined trap is listed.

Deleting Trap Destinations

To delete a trap destination, follow these steps:

Step 1   Choose **Services > Mobility Services Engines**.

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   Select the check box next to the trap destination entry that you want to delete.

Step 5   From the Select a command drop-down list, choose **Add Trap Destination**. Click **Go**.

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

Viewing and Configuring Advanced Parameters

In the Prime Infrastructure Advanced Parameters page, you can view general system level settings of the Mobility Services Engine and configure monitoring parameters.

- See the Viewing Advanced Parameter Settings to view current system- level advanced parameters.

- See the Initiating Advanced Commands to modify the current system- level advanced parameters or initiate advanced commands such as system reboot, system shut down, or clear a configuration file.

Viewing Advanced Parameter Settings

To view the advanced parameter settings of the Mobility Services Engine, follow these steps:

Step 1   Choose **Services > Mobility Services Engines**.

Step 2   Click the name of a Mobility Services Engine to view its status.

Step 3   Choose **System** > **Advanced Parameters**. The Advanced Parameters page appears.

Initiating Advanced Parameters

The Advanced Parameters page of the Prime Infrastructure enables you to set the number of days events are kept and set session time out values. It also enables you to initiate a system reboot or shut down, or clear the system database.

Note   You can use the Prime Infrastructure to modify troubleshooting parameters for a Mobility Services Engine or a location appliance.

In the Advanced Parameters page, you can use the Prime Infrastructure as follows:

- To set how long events are kept and how long before a session times out.

    For more information, see the Configuring Advanced Parameters.

- To initiate a system reboot or shutdown, or clear the system database.

    For more information, see the Initiating Advanced Commands.

Configuring Advanced Parameters

To configure advanced parameters, follow these steps:

Step 1   Choose **Services > Mobility Services Engines**.

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

Step 3   From the left sidebar menu, choose **System > Advanced Parameters**.

Step 4   View or modify the advanced parameters as necessary.

- General Information
    - Product Name
    - Version
    - Started At
    - Current Server Time

◦ Hardware Resets

◦ Active Sessions

• Advanced Parameters

Caution   Enable advanced debugging only under the guidance of Cisco TAC personnel because advanced debugging slows the mobility service down.

◦ Number of Days to keep Events—Enter the number of days to keep logs. Change this value as required for monitoring and troubleshooting.

◦ Session Timeout—Enter the number of minutes before a session times out. Change this value as required for monitoring and troubleshooting. Currently this option appears dimmed.

• Cisco UDI

◦ Product Identifier (PID)—The product ID of the MSE.

◦ Version Identifier (VID)—The version number of the MSE.

◦ Serial Number (SN)—Serial number of the MSE.

• Advanced Commands

◦ Reboot Hardware—Click to reboot the mobility services hardware. See the Rebooting or Shutting Down a System, on page 46 for more information.

◦ Shutdown Hardware—Click to turn off the mobility services hardware. See the Rebooting or Shutting Down a System, on page 46 for more information.

◦ Clear Database—Click to clear the mobility services database. See the Clearing the System Database, on page 46 for more information. Unselect the **Retain current service assignments in Prime Infrastructure** check box to remove all existing service assignments from the Prime Infrastructure and MSE. The resources must be reassigned in the **Services** > **Synchronize Services** page. By default, this option is selected.

Step 5   Click **Save** to update the Prime Infrastructure and MSE databases.

Initiating Advanced Commands

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

• Rebooting or Shutting Down a System

• Clearing the System Database

Rebooting or Shutting Down a System

To reboot or shut down a Mobility Services Engine, follow these steps:

Step 1   Choose **Services > Mobility Services Engines**.

Step 2   Click the name of a Mobility Services Engine you want to reboot or shut down.

Step 3   Choose **System > Advanced Parameters**.

Step 4   In the Advanced Commands group box, click the appropriate button (**Reboot Hardware** or **Shutdown Hardware**). Click **OK** in the confirmation dialog box to initiate either the reboot or shutdown process. Click **Cancel** to stop the process.

Clearing the System Database

To clear a Mobility Services Engine configuration and restore its factory defaults, follow these steps:

Step 1   Choose **Services > Mobility Services Engines**.

Step 2   Click the name of the Mobility Services Engine you want to configure.

Step 3   Choose **System > Advanced Parameters**.

Step 4   In the Advanced Commands group box, unselect the **Retain current service assignments in Prime Infrastructure** check box to remove all existing service assignments from the Prime Infrastructure and MSE.
The resources must be reassigned in the Services > Synchronize Services page. By default, this option is selected.

Step 5   In the Advanced Commands group box, click **Clear Database**.

Step 6   Click **OK** to clear the Mobility Services Engine database.

CHAPTER 5

Working with Maps

Maps provide a summary view of all your managed systems on campuses, buildings, outdoor areas, and floors.

About Maps

The Next Generation Maps feature is enabled by default.

The Next Generation Maps feature provides you the following benefits:

- Displays large amount of information on the map. When you have various clients, interferers, and access points, they may clutter the display on the Prime Infrastructure map pages and sometimes pages load slowly. The Release 7.3 introduces clustering and layering of information. Information cluster reduces clutter at the high level and reveals more information when you click an object. For details, see the Monitoring the Floor Area, on page 76.

- Simplifies and accelerates the process of adding APs to the map. In the legacy maps, the process of adding access points to maps was manual and tedious. With Release 7.3, you can use the automated hierarchy creation to add and name the access points. For details, see the Using the Automatic Hierarchy to Create Maps, on page 80.

- Provides high quality map images with easy navigation and zoom/pan controls. In the legacy maps, the map image quality was low and the navigating, zooming, and panning was slow. With Release 7.3, you can use the next-generation tile-aware map engine to load maps faster and zoom/pan easily. The Next

Generation Maps enables you to load high resolution maps faster and navigate around the map easily. For details, see the Planning and Zooming with Next Generation Maps, on page 76.

Adding a Building to a Campus Map

To add a building to a campus map in the Prime Infrastructure database, follow these steps:

Step 1 Choose **Design** > **Site Maps** to display the Maps page.

Step 2 Click the desired campus. The Site Maps > Campus Name page appears.

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

Step 4 In the Campus Name > New Building page, follow these steps to create a virtual building in which you can organize related floor plan maps:

  1 Enter the building name.

  2 Enter the building contact name.

  3 Enter the number of floors and basements.

  4 Enter the horizontal position (distance from the corner of the building rectangle to the left edge of the campus map) and the vertical position (distance from the corner of the building rectangle to the top edge of the campus map) in feet.

   Note To change the unit of measurement (feet or meters), choose **Design** > **Site Maps**, and choose **Properties** from the Select a command drop-down list.

  5 Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.

   Note The horizontal and vertical span should be larger than or the same size as any floors that you might add later.

   Tip You can also use **Ctrl-click** to resize the bounding area in the upper-left corner of the campus map. As you change the size of the bounding area, the horizontal span and the vertical span parameters of the building change to match your actions.

  6 Click **Place** to put the building on the campus map. The Prime Infrastructure creates a building rectangle scaled to the size of the campus map.

  7 Click the building rectangle and drag it to the desired position on the campus map.

   Note After adding a new building, you can move it from one campus to another without having to recreate it.

  8 Click Save to save this building and its campus location to the database. The Prime Infrastructure saves the building name in the rectangle on the campus map.

   Note A hyperlink associated with the building takes you to the corresponding Map page.

Step 5 (Optional) To assign location presence information for the new outdoor area, do the following:

  1 Choose **Edit Location Presence Info** from the Select a command drop-down list. Click **Go**. The Location Presence page appears.

   2   Click the **Civic Address** or **Advanced** tab.

- Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.

- Advanced identifies the campus with expanded civic information such as neighborhood, city division, country, and postal community name.

Note   Each selected field is inclusive of all of those above it. For example, if you choose Advanced, it can also provide civic location information upon client demand. The selected setting must match what is set on the location server level (Services > Mobility Services).

   3   By default, the Override Child's Presence Information check box is selected. There is no need to alter this setting for standalone buildings.

Step 6   Click **Save**.

Adding Floor Areas

This section describes how to add floor plans to either a campus building or a standalone building in the Prime Infrastructure database.

Adding Floor Areas to a Campus Building

Note   Use the zoom controls at the top of the campus image to enlarge or decrease the size of the map view and to hide or show the map grid (which displays the map size in feet or meters).

To add a floor area to a campus building, follow these steps:

Step 1   Save your plan maps in .PNG, .JPG, .JPEG, or .GIF format.

Note   The maps can be of any size because Prime Infrastructure automatically resizes the maps to fit the workspace.

Note   If there are problems converting the auto-cad file, an error message is displayed. The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .png. If the native library cannot be loaded, the Prime Infrastructure displays an "unable to convert the auto-cad file" message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls Prime Infrastructure installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occurs, you have to install the required libraries and restart Prime Infrastructure.

Cisco Wireless Intrusion Prevention System Configuration Guide, Release 8.0

Note   The floor map image is enhanced for zooming and panning. The floor image is not visible completely until this operation is complete. You can zoom in and out to view the complete map image. For example, if you have a high resolution image (near 181 megapixels) whose size is approximately 60 megabytes, it may take two minutes to appear on the map.

Step 2   Choose **Design** > **Site Maps**.

Step 3   From the Maps Tree View or the Design > Site Maps list, choose the applicable campus building to open the Building View page.

Step 4   Hover your mouse cursor over the name within an existing building rectangle to highlight it.

Note   You can also access the building from the Campus View page. In the Campus View page, click the building name to open the Building View page.

Step 5   From the Select a command drop-down list, choose **New Floor Area**.

Step 6   Click **Go**. The New Floor Area page appears.

Step 7   In the New Floor Area page, follow these steps to add floors to a building in which to organize related floor plan maps:

1   Enter the floor area and contact names.

2   Choose the floor or basement number from the Floor drop-down list.

3   Choose the floor or basement type (RF Model).

4   Enter the floor-to-floor height in feet.

    Note   To change the unit of measurement (feet or meters), choose **Design** > **Site Maps**, and choose **Properties** from the Select a command drop-down list.

5   Select the **Image or CAD File** check box.

6   Browse to and choose the desired floor or basement image or CAD filename, and click **Open**.

    Note   If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

    Tip   We do not recommend a .JPEG (.JPG) format for an auto-cad conversion. Unless a JPEG is specifically required, use .PNG or .GIF format for higher quality images.

7   Click **Next**. At this point, if a CAF file was specified, a default image preview is generated and loaded.

    Note   The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, Prime Infrastructure displays the following error: "Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library." For more information see Prime Infrastructure online help or Prime Infrastructure documentation.

    The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

    Note   When you choose the floor or basement image filename, the Prime Infrastructure displays the image in the building-sized grid.

    Note   The maps can be of any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

    Note   The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.

8   If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.

    Enter the remaining parameters for the floor area.

9   Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.

10 Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

Note The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure database.

11 If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

Tip Use **Ctrl-click** to resize the image within the building-sized grid.

12 If desired, select the **Launch Map Editor after floor creation** check box to rescale the floor and draw walls.

13 Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Design > Site Maps list.

Note Use different floor names in each building. If you are adding more than one building to the campus map, do not use a floor name that exists in another building. This overlap causes incorrect mapping information between a floor and a building.

14 Click any of the floor or basement images to view the floor plan or basement map.

Note You can zoom in or out to view the map at different sizes and you can add access points.

Adding Floor Plans to a Standalone Building

To add floor plans to a standalone building, follow these steps:

Step 1 Save your floor plan maps in .PNG, .JPG, or .GIF format.
Note The maps can be of any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

Step 2 Browse to and import the floor plan maps from anywhere in your file system. You can import CAD files in DXF or DWG formats or any of the formats you created in Step 1.
Note If there are problems converting the auto-cad file, an error message is displayed. the Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. If the native library cannot be loaded, the Prime Infrastructure displays an "unable to convert the auto-cad file" message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls the Prime Infrastructure installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occurs, you must install the required libraries and restart the Prime Infrastructure.

Step 3 Choose **Design** > **Site Maps**.
Step 4 From the Maps Tree View or the Design > Site Maps left sidebar menu, choose the desired building to display the Building View page.
Step 5 From the Select a command drop-down list, choose **New Floor Area**.
Step 6 Click **Go**.
Step 7 In the New Floor Area page, add the following information:

- Enter the floor area and contact names.

Cisco Wireless Intrusion Prevention System Configuration Guide, Release 8.0

• Choose the floor or basement number from the Floor drop-down list.

• Choose the floor or basement type (RF Model).

• Enter the floor-to-floor height in feet

• Select the **Image or CAD File** check box.

• Browse to and choose the desired floor or basement Image or CAD file, and click **Open**.

Note	If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.
Tip	A .JPEG (.JPG) format is not recommended for an auto-cad conversion. Unless a .JPEG is specifically required, use a .PNG or .GIF format for higher quality images.

Step 8   Click **Next**. At this point, if a CAD file was specified, a default image preview is generated and loaded.

Note	The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, the Prime Infrastructure displays the following error: "Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library. For more information, see the Prime Infrastructure online help or the Prime Infrastructure documentation".

The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

Note	When you choose the floor or basement image filename, the Prime Infrastructure displays the image in the building-sized grid.
Note	The maps can be any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.
Note	The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.

If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.

Step 9   Enter the remaining parameters for the floor area.

• Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio

• Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

Note	The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure Prime Infrastructure database.

• If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

Note	Use **Ctrl-click** to resize the image within the building-sized grid.

• Adjust the floor characteristics with the Prime Infrastructure map editor by selecting the check box next to Launch Map Editor. See the "Using the Map Editor" section on page 10-17 for more information regarding the map editor feature.

Step 10   Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Design > Site Maps list.

Step 11   Click any of the floor or basement images to view the floor plan or basement map.

Note	You can zoom in or out to view the map at different sizes and you can add access points.

Adding a Campus Map

To add a single campus map to the Prime Infrastructure database, follow these steps:

Step 1 Save the map in.PNG,.JPG,.JPEG, or.GIF format.

Note The map can be of any size because the Prime Infrastructure automatically resizes the map to fit the working areas.

Step 2 Browse to and import the map from anywhere in your file system.

Step 3 Choose **Design** > **Site Maps** to display the Maps page.

Step 4 From the Select a command drop-down list, choose **New Campus**, and click **Go**.

Step 5 In the Maps > New Campus page, enter the campus name and campus contact name.

Step 6 Browse to and choose the image filename containing the map of the campus, and click **Open**.

Step 7 Select the **Maintain Aspect Ratio** check box to prevent length and width distortion when the Prime Infrastructure resizes the map.

Step 8 Enter the horizontal and vertical span of the map in feet.

Note To change the unit of measurement (feet or meters), choose **Design** > **Site Maps** and choose **Properties** from the Select a command drop-down list. The horizontal and vertical span should be larger than any building or floor plan to be added to the campus.

Step 9 Click **OK** to add this campus map to the Prime Infrastructure database. The Prime Infrastructure displays the Maps page, which lists maps in the database, map types, and campus status.

Step 10 (Optional) To assign location presence information, click the newly created campus link in the Design > Site Maps page.

Configuring Buildings

You can add buildings to the Prime Infrastructure database regardless of whether you have added campus maps to the database. This section describes how to add a building to a campus map or a standalone building (one that is not part of a campus) to the Prime Infrastructure database.

- Adding a Building to a Campus Map
- Viewing a Building, on page 56
- Editing a Building, on page 57
- Deleting a Building, on page 57
- Moving a Building, on page 58

Adding a Building to a Campus Map

To add a building to a campus map in the NCS database, follow these steps:

Step 1 Choose **Monitor > Site Maps** to display the Maps page.

Step 2 Click the desired campus. The Site Maps > Campus Name page appears.

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

Step 4 In the Campus Name > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:

a) Enter the building name.

b) Enter the building contact name.

c) Enter the number of floors and basements.

d) Enter the horizontal position (distance from the corner of the building rectangle to the left edge of the campus map) and the vertical position (distance from the corner of the building rectangle to the top edge of the campus map) in feet.

Note To change the unit of measurement (feet or meters), choose Monitor > Site Maps, and choose Properties from the Select a command drop-down list.

e) Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.

Note The horizontal and vertical span should be larger than or the same size as any floors that you might add later.

Tip You can also use Ctrl-click to resize the bounding area in the upper-left corner of the campus map. As you change the size of the bounding area, the Horizontal Span and Vertical Span parameters of the building change to match your actions.

f) Click **Place** to put the building on the campus map. The NCS creates a building rectangle scaled to the size of the campus map.

g) Click the building rectangle and drag it to the desired position on the campus map.

Note After adding a new building, you can move it from one campus to another without having to recreate it.

h) Click **Save** to save this building and its campus location to the database. The NCS saves the building name in the building rectangle on the campus map.

Note A hyperlink associated with the building takes you to the corresponding Map page.

Step 5 *(Optional)* To assign location presence information for the new outdoor area, do the following:

a) Choose **Edit Location Presence Info** from the Select a command drop-down list. Click **Go**. The Location Presence page appears.

Note By default, the Presence Info check box of the Override Child Element is selected. This option should remain selected if you want to propagate the campus location to all buildings and floors on that campus. When adding buildings to the campus map, you can import the campus location information. The campus address cannot be imported to a building if the check box is unselected. ?This option should be unselected if you want to assign building-specific addresses to buildings on its campus rather than one campus address to all.

b) Click the **Civic Address**, **GPS Markers**, or **Advanced** tab.

• Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.

• GPS Markers identify the campus by longitude and latitude.

- Advanced identifies the campus with expanded civic information such as neighborhood, city division, country, and postal community name.

  Note Each selected field is inclusive of all of those above it. For example, if you choose Advanced, it can also provide GPS and Civic location information upon client demand. The selected setting must match what is set on the location server level (Services > Mobility Services).

  Note If a client requests location information such as GPS Markers for a campus, building, floor, or outdoor area that is not configured for that field, an error message is returned.

c) By default, the **Override Child's Presence Information** check box is selected. There is no need to alter this setting for standalone buildings.

Step 6 Click **Save**.

Adding a Standalone Building

To add a standalone building to the Prime Infrastructure database, follow these steps:

Step 1 Choose **Monitor > Site Maps** to display the Maps page.

Step 2 From the Select a command drop-down list, choose **New Building**, and click **Go**

Step 3 In the Maps > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:

a) Enter the building name.

b) Enter the building contact name.

  Note After adding a new building, you can move it from one campus to another without having to recreate it.

c) Enter the number of floors and basements.

d) Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.

  Note To change the unit of measurement (feet or meters), choose **Monitor** > **Site Maps**, and choose **Properties** from the Select a command drop-down list.

  Note The horizontal and vertical span should be larger than or the same size as any floors that you might add later.

e) Click OK to save this building to the database.

Step 4 *(Optional)* To assign location presence information for the new building, do the following:

a) Choose **Location Presence** from the Select a command drop-down list. Click **Go**. The Location Presence page appears.

b) Click the **Civic**, **GPS Markers**, or **Advanced** tab.

- Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.

- GPS Markers identify the campus by longitude and latitude.

- Advanced identifies the campus with expanded civic information such as neighborhood, city division, county, and postal community name.

Cisco Wireless Intrusion Prevention System Configuration Guide, Release 8.0

> **Note** Each selected field is inclusive of all of those above it. For example, if you select Advanced, it can also provide GPS and Civic location information upon client demand. The selected setting must match what is set on the location server level (Services > Mobility Services).
>
> **Note** If a client requests location information such as GPS Markers for a campus, building, floor, or outdoor area that is not configured for that field, an error message is returned.

c) By default, the Presence Info check box of the Override Child Element is selected. This option should remain selected if you want to propagate the campus location to all buildings and floors on that campus. When adding buildings to the campus map, you can import the location information. The campus address cannot be imported to a building if the check box is unselected. This option should be deselected if you want to assign building-specific addresses to buildings on its campus rather than one campus address to all.

Step 5 Click **Save**.

> **Note** The standalone buildings are automatically placed in System Campus.

Viewing a Building

To view a current building map, follow these steps:

Step 1 Choose **Monitor** > **Site Maps**.

Step 2 Click the name of the building map to open its details page. The Building View page provides a list of floor maps and map details for each floor.

> **Note** From the Building View page, you can click the Floor column heading to sort the list ascending or descending by floor.

The map details include the following:

- Floor area

- Floor index—Indicates the floor level. A negative number indicates a basement floor level.

- Contact

- Status—Indicates the most serious level of alarm on an access point located on this map or one of its children.

- Number of total access points located on the map.

- Number of 802.11a/n and 802.11b/g/n radios located on the map.

- Number of out of service (OOS) radios.

- Number of clients—Click the number link to view the Monitor > Clients page.

Step 3 The Select a command drop-down list provides the following options:

- New Floor Area—See the Adding a Building to a Campus Map for more information.

- Edit Building—See the Editing a Building, on page 57 for more information.

- Delete Building—See the Deleting a Building, on page 57 for more information.

Editing a Building

To edit a current building map, follow these steps:

Step 1   Choose **Monitor** > **Site Maps**.

Step 2   Click the name of the building map to open its details page.

Step 3   From the Select a command drop-down list, choose **Edit Building**.

Step 4   Make any necessary changes to Building Name, Contact, Number of Floors, Number of Basements, and Dimensions (feet).

    Note   To change the unit of measurement (feet or meters), choose **Monitor** > **Site Maps**, and choose **Properties** from the Select a command drop-down list.

Step 5   Click **OK**.

Deleting a Building

To delete a current building map, follow these steps:

Step 1   Choose **Monitor** > **Site Maps**.

Step 2   Select the check box for the building that you want to delete.

Step 3   Click **Delete** at the bottom of the map list (or choose **Delete Maps** from the Select a command drop-down list, and click **Go**).

Step 4   Click **OK** to confirm the deletion.

    Note   Deleting a building also deletes all of its container maps. The access points from all deleted maps are moved to an Unassigned state.

Moving a Building

To move a building to a different campus, follow these steps:

Step 1 Choose **Monitor** > **Site Maps**.

Step 2 Select the check box of the applicable building.

Step 3 From the Select a command drop-down list, choose **Move Buildings**.

Step 4 Click **Go**.

Step 5 Choose the **Target Campus** from the drop-down list.

Step 6 Select the buildings that you want to move. Unselect any buildings that remain in their current location.

Step 7 Click **OK**.

Adding Floor Areas

This section describes how to add floor plans to either a campus building or a standalone building in the Prime Infrastructure database.

Adding Floor Areas to a Campus Building

Note Use the zoom controls at the top of the campus image to enlarge or decrease the size of the map view and to hide or show the map grid (which displays the map size in feet or meters).

To add a floor area to a campus building, follow these steps:

Step 1 Save your plan maps in .PNG, .JPG, ,JPEG, or .GIF format.

Note The maps can be of any size because Prime Infrastructure automatically resizes the maps to fit the workspace.

Note If there are problems converting the auto-cad file, an error message is displayed. The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .png. If the native library cannot be loaded, the Prime Infrastructure displays an "unable to convert the auto-cad file" message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls Prime Infrastructure installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occurs, you have to install the required libraries and restart Prime Infrastructure.

Note	The floor map image is enhanced for zooming and panning. The floor image is not visible completely until this operation is complete. You can zoom in and out to view the complete map image. For example, if you have a high resolution image (near 181 megapixels) whose size is approximately 60 megabytes, it may take two minutes to appear on the map.

Step 2   Choose **Design** > **Site Maps**.

Step 3   From the Maps Tree View or the Design > Site Maps list, choose the applicable campus building to open the Building View page.

Step 4   Hover your mouse cursor over the name within an existing building rectangle to highlight it.

Note	You can also access the building from the Campus View page. In the Campus View page, click the building name to open the Building View page.

Step 5   From the Select a command drop-down list, choose **New Floor Area**.

Step 6   Click **Go**. The New Floor Area page appears.

Step 7   In the New Floor Area page, follow these steps to add floors to a building in which to organize related floor plan maps:

1. Enter the floor area and contact names.

2. Choose the floor or basement number from the Floor drop-down list.

3. Choose the floor or basement type (RF Model).

4. Enter the floor-to-floor height in feet.

Note	To change the unit of measurement (feet or meters), choose **Design** > **Site Maps**, and choose **Properties** from the Select a command drop-down list.

5. Select the **Image or CAD File** check box.

6. Browse to and choose the desired floor or basement image or CAD filename, and click **Open**.

Note	If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.
Tip	We do not recommend a .JPEG (.JPG) format for an auto-cad conversion. Unless a JPEG is specifically required, use .PNG or .GIF format for higher quality images.

7. Click **Next**. At this point, if a CAF file was specified, a default image preview is generated and loaded.

Note	The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, Prime Infrastructure displays the following error: "Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library." For more information see Prime Infrastructure online help or Prime Infrastructure documentation.
	The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.
Note	When you choose the floor or basement image filename, the Prime Infrastructure displays the image in the building-sized grid.
Note	The maps can be of any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.
Note	The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.

8. If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.

    Enter the remaining parameters for the floor area.

9. Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.

10 Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

> **Note** The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure database.

11 If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

> **Tip** Use **Ctrl-click** to resize the image within the building-sized grid.

12 If desired, select the **Launch Map Editor after floor creation** check box to rescale the floor and draw walls.

13 Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Design > Site Maps list.

> **Note** Use different floor names in each building. If you are adding more than one building to the campus map, do not use a floor name that exists in another building. This overlap causes incorrect mapping information between a floor and a building.

14 Click any of the floor or basement images to view the floor plan or basement map.

> **Note** You can zoom in or out to view the map at different sizes and you can add access points.

Adding Floor Plans to a Standalone Building

To add floor plans to a standalone building, follow these steps:

Step 1 Save your floor plan maps in .PNG, .JPG, or .GIF format.
> **Note** The maps can be of any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

Step 2 Browse to and import the floor plan maps from anywhere in your file system. You can import CAD files in DXF or DWG formats or any of the formats you created in Step 1.
> **Note** If there are problems converting the auto-cad file, an error message is displayed. the Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. If the native library cannot be loaded, the Prime Infrastructure displays an "unable to convert the auto-cad file" message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls the Prime Infrastructure installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occurs, you must install the required libraries and restart the Prime Infrastructure.

Step 3 Choose **Design** > **Site Maps**.

Step 4 From the Maps Tree View or the Design > Site Maps left sidebar menu, choose the desired building to display the Building View page.

Step 5 From the Select a command drop-down list, choose **New Floor Area**.

Step 6 Click **Go**.

Step 7 In the New Floor Area page, add the following information:

- Enter the floor area and contact names.

• Choose the floor or basement number from the Floor drop-down list.

• Choose the floor or basement type (RF Model).

• Enter the floor-to-floor height in feet

• Select the **Image or CAD File** check box.

• Browse to and choose the desired floor or basement Image or CAD file, and click **Open**.

Note   If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

Tip   A .JPEG (.JPG) format is not recommended for an auto-cad conversion. Unless a .JPEG is specifically required, use a .PNG or .GIF format for higher quality images.

Step 8   Click **Next**. At this point, if a CAD file was specified, a default image preview is generated and loaded.

Note   The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, the Prime Infrastructure displays the following error: "Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library. For more information, see the Prime Infrastructure online help or the Prime Infrastructure documentation".

The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

Note   When you choose the floor or basement image filename, the Prime Infrastructure displays the image in the building-sized grid.

Note   The maps can be any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

Note   The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.

If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.

Step 9   Enter the remaining parameters for the floor area.

• Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio

• Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

Note   The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure Prime Infrastructure database.

• If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

Note   Use **Ctrl-click** to resize the image within the building-sized grid.

• Adjust the floor characteristics with the Prime Infrastructure map editor by selecting the check box next to Launch Map Editor. See the "Using the Map Editor" section on page 10-17 for more information regarding the map editor feature.

Step 10   Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Design > Site Maps list.

Step 11   Click any of the floor or basement images to view the floor plan or basement map.

Note   You can zoom in or out to view the map at different sizes and you can add access points.

Configuring Floor Settings

You can modify the appearance of the floor map by selecting or unselecting various floor settings check boxes. The selected floor settings appears in the map image.

Note Depending on whether or not a Mobility Services Engine is present in the Prime Infrastructure, some of the floor settings might not be displayed. Clients, 802.11 Tags, Rogue APs, Adhoc Rogues, Rouge Clients, and Interferers are visible only if an MSE is present in the Prime Infrastructure

The Floor Settings options include the following:

- Access Points—See the Filtering Access Point Floor Settings for more information.

- AP Heatmaps—See the Filtering Access Point Heatmap Floor Settings for more information.

- AP Mesh Info—See the Filtering AP Mesh Info Floor Settings for more information.

- Clients—See the Filtering Client Floor Settings for more information.

- 802.11 Tags—See the Filtering 802.11 Tag Floor Settings for more information.

- Rogue APs—See the Filtering Rogue AP Floor Settings for more information.

- Rogue Adhocs—See the Filtering Rogue Adhoc Floor Settings for more information.

- Rogue Clients—See the Filtering Rogue Client Floor Settings for more information.

- Coverage Areas

- Location Regions

- Rails

- Markers

- Chokepoints

- Wi-Fi TDOA Receivers

- Interferers—See the Filtering Interferer Settings for more information.

- wIPS Attackers—See the Filtering wIPS Attacker Floor Settings, on page 73 for more information.

Use the blue arrows to access floor setting filters for access points, access point heatmaps, clients, 802.11 tags, rogue access points, rogue adhocs, and rogue clients. When filtering options are selected, click OK.

Use the Show MSE data within last drop-down list to choose the timeframe for Mobility Services Engine data. Choose to view Mobility Services Engine data from a range including the past two minutes up to the past 24 hours. This option only appears if a Mobility Services Engine is present on the Prime Infrastructure.

Click **Save** Settings to make the current view and filter settings your new default for all maps.

Defining Inclusion and Exclusion Regions on a Floor

To further refine location calculations on a floor, you can define the areas that are included (inclusion areas) in the calculations and those areas that are not included (exclusion areas).

For example, you might want to exclude areas such as an atrium or stairwell within a building but include a work area (such as cubicles, labs, or manufacturing floors).

Cisco 1000 Series Lightweight Access Point Icons

The icons indicate the present status of an access point. The circular part of the icon can be split in half horizontally. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.

Note   When the icon is representing 802.11a/n and 802.11b/n, the top half displays the 802.11a/n status, and the bottom half displays the 802.11b/g/n status. When the icon is representing only 802.11b/g/n, the whole icon displays the 802.11b/g/n status. The triangle indicates the more severe color.

The below table shows the icons used in the Prime Infrastructure user interface Map displays.

Table 11: Access Points Icons Description

Icon	Description
	The green icon indicates an access point (AP) with no faults. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio.
	The yellow icon indicates an access point with a minor fault. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio. **Note** A flashing yellow icon indicates that there has been an 802.11a or 802.11b/g interference, noise, coverage, or load Profile Failure. A flashing yellow icon indicates that there have been 802.11a and 802.11b/g profile failures.
	The red icon indicates an access point (AP) with a major or critical fault. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio.
	The dimmed icon with a question mark in the middle represents an unreachable access point. It is gray because its status cannot be determined.

Icon	Description
	The dimmed icon with no question mark in the middle represents an unassociated access point.
	The icon with a red "x" in the center of the circle represents an access point that has been administratively disabled.
	The icon with the top half green and the lower half yellow indicates that the optional 802.11a Cisco Radio (top) has no faults, and the 802.11b/g Cisco Radio (bottom) has a minor fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half green and the lower half red indicates that the optional 802.11a Cisco Radio (top) is operational with no faults, and the 802.11b/g Cisco Radio (bottom) has a major or critical fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half yellow and the lower half red indicates that the optional 802.11a Cisco Radio (top) has a minor fault, and the 802.11b/g Cisco Radio (bottom) has a major or critical fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half yellow and the lower half green indicates that the optional 802.11a Cisco Radio (top) has a minor fault, and the 802.11b/g Cisco Radio (bottom) is operational with no faults. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half red and the lower half green indicates that the optional 802.11a Cisco Radio (top) has a major or critical fault, and the 802.11b/g Cisco Radio (bottom) is operational with no faults. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half red and the lower half yellow indicates that the optional 802.11a Cisco Radio (top) has major or critical faults, and the 802.11b/g Cisco Radio (bottom) has a minor fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.

Icon	Description
	The icon with a red "x" on the top half (optional 802.11a) shows that the indicated Cisco Radio has been administratively disabled. There are six color coding possibilities as shown.

Each of the access point icons includes a small black arrow that indicates the direction in which the internal Side A antenna points.

The below table shows some arrow examples used in the Prime Infrastructure user interface map displays.

Table 12: Arrows

Arrow Examples	Direction
	Zero degrees, or to the right on the map.
	45 degrees, or to the lower right on the map.

Arrow Examples	Direction
	90 degrees, or down on the map.
These examples show the first three 45-degree increments allowed, with an additional five at 45-degree increments.	

Filtering Access Point Floor Settings

If you enable the access point floor setting and then click the blue arrow to the right of the floor settings, the Access Point Filter dialog box appears with filtering options.

Access point filtering options include the following:

- Show—Select this radio button to display the radio status or the access point status.

  Note Because the access point icon color is based on the access point status, the icon color might vary depending on the status selected. The default on floor maps is radio status.

- Protocol—From the drop-down list, choose which radio types to display (802.11a/n, 802.11b/g/n, or both).

  Note The displayed heatmaps correspond to the selected radio type(s).

- Display—From the drop-down list, choose what identifying information is displayed for the access points on the map image.

  - Channels—Displays the Cisco Radio channel number or Unavailable (if the access point is not connected).

    Note The available channels are defined by the country code setting and are regulated by country. See the following URL for more information:?http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html

  - TX Power Level—Displays the current Cisco Radio transmit power level (with 1 being high) or Unavailable (if the access point is not connected).

Note The power levels differ depending on the type of access point. The 1000 series access points accept a value between 1 and 5, the 1230 access points accept a value between 1 and 7, and the 1240 and 1100 series access points accept a value between 1 and 8.

The below table lists the transmit power level numbers and their corresponding power setting.

Table 13: Transmit Power Level Values

Transmit Power?Level Number	Power Setting
1	Maximum power allowed per country code setting
2	50% power
3	25% power
4	12.5 to 6.25% power
5	6.25 to 0.195% power

Note The power levels are defined by the country code setting and are regulated by country. See the following URL for more information:?http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html

- Channel and Tx Power—Displays both the channel and transmit power level (or Unavailable if the access point is not connected).

- Coverage Holes—Displays a percentage of clients whose signal has become weaker until the client lost its connection, Unavailable for unconnected access points, or MonitorOnly for access points in monitor-only mode.

Note Coverage holes are areas in which clients cannot receive a signal from the wireless network. When you deploy a wireless network, you must consider the cost of the initial network deployment and the percentage of coverage hole areas. A reasonable coverage hole criterion for launch is between 2 and 10 percent. This means that between two and ten test locations out of 100 random test locations might receive marginal service. After launch, Cisco Unified Wireless Network Solution Radio Resource Management (RRM) identifies these coverage hole areas and reports them to the IT manager, who can fill holes based on user demand.

- MAC Addresses—Displays the MAC address of the access point, whether or not the access point is associated to a controller.

- Names—Displays the access point name. This is the default value.

- Controller IP—Displays the IP address of the controller to which the access point is associated or Not Associated for disassociated access points.

- Utilization—Displays the percentage of bandwidth used by the associated client devices (including receiving, transmitting, and channel utilization). Displays Unavailable for disassociated access points and MonitorOnly for access points in monitor-only mode.

- Profiles—Displays the load, noise, interference, and coverage components of the corresponding operator-defined thresholds. Displays Okay for thresholds not exceeded, Issue for exceeded thresholds, or Unavailable for unconnected access points.

> **Note** Use the Profile Type drop-down list to choose Load, Noise, Interference, or Coverage.

- CleanAir Status—Displays the CleanAir status of the access point and whether or not CleanAir is enabled on the access point.

- Average Air Quality—Displays the average air quality on this access point. The details include the band and the average air quality.

- Minimum Air Quality—Displays the minimum air quality on this access point. The details include the band and the minimum air quality.

- Average and Minimum Air Quality—Displays the average and minimum air quality on this access point. The details include the band, average air quality, and minimum air quality.

- Associated Clients—Displays the number of associated clients, Unavailable for unconnected access points or MonitorOnly for access points in monitor-only mode.

> **Note**

- Bridge Group Names

- RSSI Cutoff—From the drop-down list, choose the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBm.

- Show Detected Interferers—Select the check box to display all interferers detected by the access point.

- Max. Interferers/label—Choose the maximum number of interferers to be displayed per label from the drop-down list.

Click **OK** when all applicable filtering criteria are selected.

Filtering Access Point Heatmap Floor Settings

An RF heatmap is a graphical representation of RF wireless data where the values taken by variables are represented in maps as colors. The current heatmap is computed based on the RSSI prediction model, Antenna Orientation, and AP transmit power.

If you enable the Access Point Heatmap floor setting and click the blue arrow to the right of the Floor Settings, the Contributing APs dialog appears with heatmap filtering options. See the Understanding RF Heatmap Calculation for more information.

The Prime Infrastructure introduces dynamic heatmaps. When dynamic heatmaps are enabled, the Prime Infrastructure recomputes the heatmaps to represent changed RSSI values. To configure the dynamic heatmaps, see the Editing Map Properties for more information.

Access point heatmap filtering options include the following:

- Heatmap Type—Select Coverage, or Air Quality. If you choose Air Quality, you can further filter the heat map type for access points with average air quality or minimum air quality. Select the appropriate radio button.

> **Note** If you have monitor mode access points on the floor plan, you have a choice between IDS or coverage heatmap types. A coverage heatmap excludes monitor mode access points.

> **Note** Only APs in Local, FlexConnect, or Bridge mode can contribute to the Coverage and Air Quality Heatmap.

- Total APs—Displays the number of access points positioned on the map.

- Select the access point check box(es) to determine which heatmaps are displayed on the image map.

Click OK when all applicable filtering criteria are selected.

Filtering AP Mesh Info Floor Settings

> **Note** The AP Mesh Info check box only appears when bridging access points are added to the floor.

When this check box is selected, the Prime Infrastructure initiates a contact with the controllers and displays information about bridging access points. The following information is displayed:

- Link between the child and the parent access point.

- An arrow that indicates the direction from the child to parent access point.

- A color-coded link that indicates the signal-to-noise ratio (SNR). A green link represents a high SNR (above 25 dB), an amber link represents an acceptable SNR (20-25 dB), and a red link represents a very low SNR (below 20 dB).

If you enable the AP Mesh Info floor setting and click the blue arrow to the right of the floor settings, the Mesh Parent-Child Hierarchical View page appears with mesh filtering options.

You can update the map view by choosing the access points you want to see on the map. From the Quick Selections drop-down list, choose to select only root access point, various hops between the first and the fourth, or select all access points.

> **Note** For a child access point to be visible, its parent must also be selected.

Click OK when all applicable filtering criteria are selected.

Filtering Client Floor Settings

> **Note** The Clients option only appears if a mobility server is added in the Prime Infrastructure.

If you enable the Clients floor setting and click the blue arrow to the right, the Client Filter dialog box appears.

Client filtering options include the following:

- Show All Clients—Select the check box to display all clients on the map.

- Small Icons—Select the check box to display icons for each client on the map.

  > **Note** If you select the Show All Clients check box and Small Icons check box, all other drop-down list options are dimmed. ??If you unselect the Small Icons check box, you can choose if you want the label to display the MAC address, IP address, username, asset name, asset group, or asset category.??If you unselect the Show All Clients check box, you can specify how you want the clients filtered and enter a particular SSID.

- Display—Choose the client identifier (IP address, username, MAC address, asset name, asset group, or asset category) to display on the map.

- Filter By—Choose the parameter by which you want to filter the clients (IP address, username, MAC address, asset name, asset group, asset category, or controller). Once selected, type the specific device in the text box.

- SSID—Enter the client SSID in the available text box.

- Protocol—Choose All, 802.11a/n, or 802.11b/g/n from the drop-down list.

  ◦ All—Displays all the access points in the area.

  ◦ 802.11a/n—Displays a colored overlay depicting the coverage patterns for the clients with 802.11a/n radios. The colors show the received signal strength from red (−35 dBm) through dark blue (−85 dBm).

  ◦ 802.11b/g/n—Displays a colored overlay depicting the coverage patterns for the clients with 802.11b/g/n radios. The colors show the received signal strength from red (−35 dBm) through dark blue (−85 dBm). This is the default value.

- State—Choose All, Idle, Authenticated, Probing, or Associated from the drop-down list.

Click OK when all applicable filtering criteria are selected.

Filtering 802.11 Tag Floor Settings

If you enable the 802.11 Tags floor setting and then click the blue arrow to the right, the Tag Filter dialog appears.

Tag filtering options include the following:

- Show All Tags—Select the check box to display all tags on the map.

- Small Icons—Select the check box to display icons for each tag on the map.

> **Note**   If you select the Show All Tags check box and Small Icons check box, all other drop-down list options are dimmed. If you unselect the Small Icons check box, you can choose if you want the label to display MAC address, asset name, asset group, or asset category. If you unselect the Show All Tags check box, you can specify how you want the tags filtered.

- Display—Choose the tag identifier (MAC address, asset name, asset group, or asset category) to display on the map.

- Filter By—Choose the parameter by which you want to filter the clients (MAC address, asset name, asset group, asset category, or controller). Once selected, type the specific device in the text box.

Click OK when all applicable filtering criteria are selected.

Filtering Rogue AP Floor Settings

If you enable the Rogue APs floor setting and then click the blue arrow to the right, the Rogue AP filter dialog box appears.

Rogue AP filtering options include the following:

- Show All Rogue APs—Select the check box to display all rogue access points on the map.

- Small Icons—Select the check box to display icons for each rogue access point on the map.

> **Note**   If you select the Show All Rogue APs check box and Small Icons check box, all other drop-down list options are dimmed. If you unselect the Show All Rogue APs check box, you can specify how you want the rogue access points filtered.

- Show Rogue AP Zone of Impact—Select the check box to display the zone of impact for rogues. The rogue impact zone is determined by the transmission power of the Rogue AP and the number of clients associated with the rogue AP.

  ◦ The number of clients associated with the rogue AP determines the intensity of the color of the zone on the map.

  ◦ The radius of the zone of impact is determined by using the following transmission powers of the rogue AP.

Table 14: Transmission Powers

Band	Transmission Power	Assumes Tx Power
2.5 Ghz	20 dBm	18 dBm
5 Ghz	17 dBm	15 dBm

- MAC Address—If you want to view a particular MAC address, enter it in the MAC Address text box.

- State—Use the drop-down list to choose from Alert, Known, Acknowledged, Contained, Threat, or Unknown contained states.

- On Network—Use the drop-down list to specify whether or not you want to display rogue access points on the network.

Click OK when all applicable filtering criteria are selected.

Filtering Rogue Adhoc Floor Settings

If you enable the Rogue Adhocs floor setting and then click the blue arrow to the right, the Rogue Adhoc filter dialog appears.

Rogue Adhoc filtering options include the following:

- Show All Rogue Adhocs—Select the check box to display all rogue adhoc on the map.

- Small Icons—Select the check box to display icons for each rogue adhoc on the map.

Note If you select the Show All Rogue Adhocs check box and Small Icons check box, all other drop-down list options are dimmed. If you unselect the Show All Rogue Adhocs check box, you can specify how you want the rogue adhocs filtered.

- MAC Address—If you want to view a particular MAC address, enter it in the MAC Address text box.

- State—Use the drop-down list to select from Alert, Known, Acknowledged, Contained, Threat, or Unknown contained states.

- On Network—Use the drop-down list to specify whether or not you want to display rogue adhocs on the network.

Click OK when all applicable filtering criteria are selected.

Filtering Rogue Client Floor Settings

If you enable the Rogue Clients floor setting and then click the blue arrow to the right, the Rogue Clients filter dialog appears.

Rogue Clients filtering options include the following:

- Show All Rogue Clients—Select the check box to display all rogue clients on the map.

- Small Icons—Select the check box to display icons for each rogue client on the map.

> **Note** If you select the Show All Rogue Clients check box and Small Icons check box, all other drop-down list options are dimmed. If you unselect the Show All Rogue Clients check box, you can specify how you want the rogue clients filtered.

- Assoc. Rogue AP MAC Address—If you want to view a particular MAC address, enter it in the MAC Address text box.

- State—Use the drop-down list to choose from Alert, Contained, Threat, or Unknown contained states.

Click OK when all applicable filtering criteria are selected.

Filtering Interferer Settings

If you enable Interferer floor setting and then click the blue arrow to the right, the Interferers filter dialog box appears.

Interferer filtering options include the following:

- Show active interferers only—Select the check box to display all active interferers.

- Small Icons—Select the check box to display icons for each interferer on the map.

- Show Zone of Impact—Displays the approximate interference impact area. The opacity of the circle denotes its severity. A solid red circle represents a very strong interferer that likely disrupts Wi-Fi communications, a light pink circle represents a weak interferer.

- Click OK when all applicable filtering criteria are selected.

Filtering wIPS Attacker Floor Settings

If you enable the wIPS Attacker floor setting and then click the blue arrow to the right, the wIPS Attack Filter dialog box appears.

wIPS Attack filtering options include the following:

- Show All wIPS Attacks—Select the check box to display all wIPS attacks on the map.

- Small Icons—Select the check box to display icons for each wIPS attacks on the map.

> **Note** If you select the **Show All wIPS Attacks** check box and **Small Icons** check box, all other drop-down list options are dimmed. If you unselect the **Small Icons** check box, you can choose if you want the label to display the MAC address, Alarm Category, and Alarm Name. If you unselect the **Show All wIPS Attacks** check box, you can specify how you want the wIPS attacks to be filtered.

- Filter By—Choose the parameter by which you want to filter the wIPS attacks.

   ◦ MAC Address—If you want to view a particular MAC address, enter it in the MAC Address text box.

◦ Alarm Category—Choose the category of the alarm from the Alarm Category drop-down list. The possible categories are: **All Types**, **Security Penetration**, **User Authentication and Encryption**, **DoS**, **Performance Violation** and **Channel or Device overload**.

Note   The alarm name is populated bases on the alarm category selected.

◦ Alarm Name—Choose the alarm name from the Alarm Name drop-down list.

Click **OK** when all applicable filtering criteria are selected.

Figure 9: wIPS Attack Name Filtering
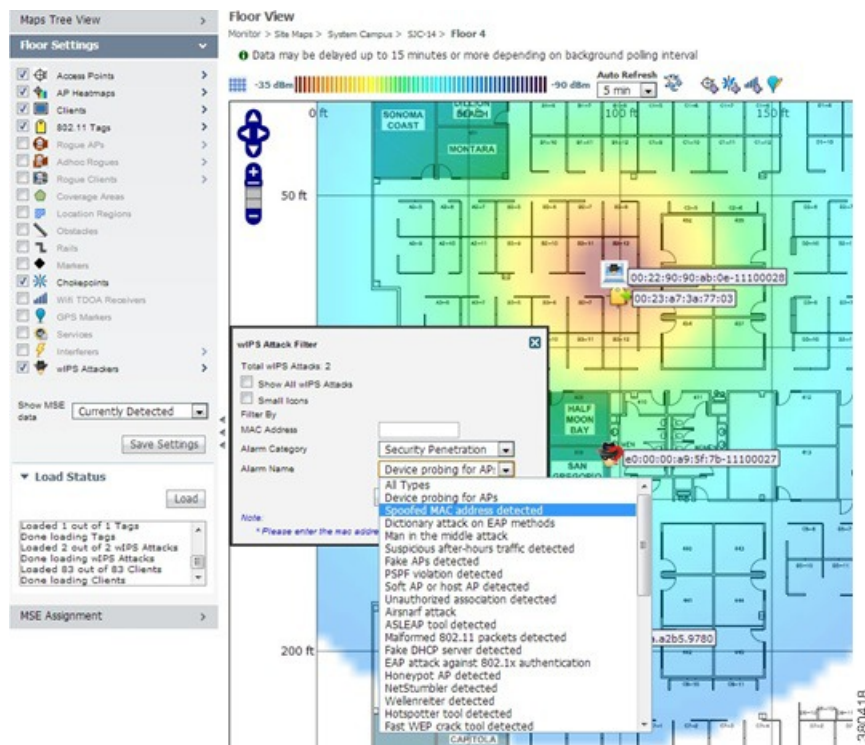
The following icons are used to distinguish between devices displayed on the map.

Figure 10: Icons

Attacker:

Victim

Unknown Device

Note   Out of all the alarms reported by wIPS, the following four alarms are detected at the wIPS server in the Mobility Services Engine (MSE) and not in the access point. For these alarms, currently there is no location information present. The list of alarms are:

- 124 Hotspotter tool detected

- 133 Day-Zero attack by device security anomaly

- 135 Day-Zero attack by WLAN security anomaly

- 138 Unauthorized association by vendor list

Import Map and AP Location Data

When converting from autonomous to lightweight access points and from WLSE to the Prime Infrastructure, one of the conversion steps is to manually reenter the access point-related information into the Prime Infrastructure. To speed up this process, you can export the information about access points from the WLSE and import it into the Prime Infrastructure.

Note   The Prime Infrastructure expects a .tar file and checks for a .tar extension before importing the file. If the file you are trying to import is not a .tar file, the Prime Infrastructure displays an error message and prompts you to import a different file.

Note   For more information on the WLSE data export functionality (WLSE Version 2.15), see the following URL: http://<WLSE_IP_ADDRESS>:1741/debug/export/exportSite.jsp.

To map properties and import a tar file containing WLSE data using the Prime Infrastructure web interface, follow these steps:

Step 1   Choose Monitor > Site Maps.

Step 2   From the Select a command drop-down list, choose Import Maps, and click Go.

Step 3   Choose the WLSE Map and AP Location Data option, and click Next.

Step 4   In the Import WLSE Map and AP Location Data page, click Browse to select the file to import.

Step 5   Find and select the .tar file to import and click Open.
The Prime Infrastructure displays the name of the file in the Import From text box.

Step 6   Click **Import**.

The CS uploads the file and temporarily saves it into a local directory while it is being processed. If the file contains data that cannot be processed, the Prime Infrastructure prompts you to correct the problem and retry. Once the file has been loaded, the Prime Infrastructure displays a report of what is added to the Prime Infrastructure. The report also specifies what cannot be added and why.

If some of the data to be imported already exists, the Prime Infrastructure either uses the existing data in the case of campuses or overwrites the existing data using the imported data in the cases of buildings and floors.

Note If there are duplicate names between a WLSE site and building combination and an Prime Infrastructure campus (or top-level building) and building combination, the Prime Infrastructure displays a message in the Pre Execute Import Report indicating that it will delete the existing building.

Step 7 Click Import to import the WLSE data.
The Prime Infrastructure displays a report indicating what was imported.

Step 8 Choose Monitor > Site Maps to view the imported data.

Monitoring the Floor Area

The floor area is the area of each floor of the building measured to the outer surface of the outer walls. This includes the area of lobbies, cellars, elevator shafts, and in multi-dwelling buildings it includes all the common spaces.

This section contains the following topics:

Planning and Zooming with Next Generation Maps

Planning

To move the map, click and hold the left mouse button and drag the map to a new place. You ca also move the map North, South, East, or West using the pan arrows. These can be found on the top left-hand corner of the map.

Note You can also perform the panning operations using the arrow keys on a keyboard.

Zooming in and out - changing the scale

The zooming levels depend upon the resolution of an image. A high resolution image may provide more zoom levels. Each zoom level is made of a different style map shown at different scales, each one showing more or less detail. Some maps will be of the same style, but at a smaller or larger scale.

To see a map with more detail you need to zoom in. You can do this using the zoom bar on the left hand side of the map. Click the + sign on the top of the zoom bar. To center and zoom in on a location, double-click the location. To see a map with less detail you need to zoom out. To do this, click the - sign on the bottom of the zoom bar.

Note   You can perform zooming operations using the mouse or keyboard. With the keyboard, click the + or - signs to zoom in or zoom out. With the mouse, use the mouse scroll wheel to zoom in or zoom out or double-click to zoom in.

Adding Access Points to a Floor Area

After you add the .PNG, .JPG, .JPEG, or .GIF format floor plan and outdoor area maps to the Prime Infrastructure database, you can position lightweight access point icons on the maps to show where they are installed in the buildings. To add access points to a floor area and outdoor area, follow these steps:

Note   There is no limit on the number of APs supported per floor by the MSE but there could be performance issues if you add more than 100 APs per floor on the Prime Infrastructure.

Step 1   Choose **Design** > **Site Maps**.

Step 2   From the Maps Tree View or the Design > Site Maps left sidebar menu, choose the applicable floor to open the Floor View page.

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

Step 4   In the Add Access Points page, select the check boxes of the access points that you want to add to the floor area.

> **Note**   If you want to search for access points, enter AP name or MAC address (Ethernet/Radio)/IP in the Search AP [Name/Mac Address (Ethernet/Radio)/IP] text box, and then click **Search**. The search is case-insensitive.

> **Note**   Only access points that are not yet assigned to any floor or outdoor area appear in the list.

> **Note**   Select the check box at the top of the list to select all access points.

Step 5   When all of the applicable access points are selected, click **OK** located at the bottom of the access point list. The Position Access Points page appears.

Each access point you have chosen to add to the floor map is represented by a gray circle (differentiated by access point name or MAC address) and is lined up in the upper left part of the floor map.

Step 6   Click and drag each access point to the appropriate location. Access points turn blue when selected.

> **Note**   When you drag an access point on the map, its horizontal and vertical position appears in the Horizontal and Vertical text boxes.

Note   The small black arrow at the side of each access point represents Side A of each access point, and each access point arrow must correspond with the direction in which the access points were installed. Side A is clearly noted on each 1000 series access point and has no relevance to the 802.11a/n radio. To adjust the directional arrow, choose the appropriate orientation from the Antenna Angle drop-down list.

When selected, the access point details are displayed on the left side of the page. Access point details include the following:

- AP Model—Indicates the model type of the selected access point.

- Protocol—Choose the protocol for this access point from the drop-down list.

- Antenna—Choose the appropriate antenna type for this access point from the drop-down list.

- Antenna/AP Image—The antenna image reflects the antenna selected from the Antenna drop-down list. Click the arrow at the top right of the antenna image to expand the image size.

- Antenna Orientation—Depending on the antenna type, enter the Azimuth and the Elevation orientations in degrees.

Note   The Azimuth option does not appear for Omnidirectional antennas because their pattern is non directional in azimuth.

Note   For internal antennas, the same elevation angle applies to both radios.

The antenna angle is relative to the map X axis. Because the origin of the X (horizontal) and Y (vertical) axes is in the upper left corner of the map, 0 degrees points side A of the access point to the right, 90 degrees points side A down, 180 degrees points side A to the left, and so on.

The antenna elevation is used to move the antenna vertically, up or down, to a maximum of 90 degrees.

Note   Make sure each access point is in the correct location on the map and has the correct antenna orientation. Accurate access point positioning is critical when you use the maps to find coverage holes and rogue access points.

See the following URL for further information about the antenna elevation and azimuth patterns: http://www.cisco.com/en/US/products/hw/wireless/ps469/tsd_products_support_series_home.html

Step 7   When you are finished placing and adjusting each access point, click **Save**.

Note   Clicking Save causes the antenna gain on the access point to correspond to the selected antenna. This might cause the radio to reset.

The Prime Infrastructure computes the RF prediction for the coverage area. These RF predictions are popularly known as *heat maps* because they show the relative intensity of the RF signals on the coverage area map.

Note   Note

This display is only an approximation of the actual RF signal intensity because it does not take into account the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions.

Note   See the "Placing Access Points" section on page 10-14 for more information on placing access points on a map.

Note   You can change the position of access points by importing or exporting a file. See the "Positioning Wi-Fi TDOA Receivers" section on page 10-30 for more information.

Placing Access Points

To determine the best location of all devices in the wireless LAN coverage areas, you need to consider the access point density and location.

Ensure that no fewer than 3 access points, and preferably 4 or 5, provide coverage to every area where device location is required. The more access points that detect a device, the better. This high level guideline translates into the following best practices, ordered by priority:

1 Most importantly, access points should surround the desired location.

2 One access point should be placed roughly every 50 to 70 linear feet (about 17 to 20 meters). This translates into one access point every 2,500 to 5000 square feet (about 230 to 450 square meters).

Note The access point must be mounted so that it is under 20 feet high. For best performance, a mounting at 10 feet would be ideal.

Following these guidelines makes it more likely that access points detect tracked devices. Rarely do two physical environments have the same RF characteristics. Users might need to adjust these parameters to their specific environment and requirements.

Note Devices must be detected at signals greater than −75 dBm for the Cisco WLCs to forward information to the location appliance. No fewer than three access points should be able to detect any device at signals below −75 dBm.

Note   If you have a ceiling-mounted AP with an integrated omni-directional antenna, the antenna orientation does not really need to be set in the Prime Infrastructure. However, if you mount that same AP on the wall, you must set the antenna orientation to 90 degrees. See Placing Access Points, on page 79 for information on orientation of the access points.

Table 15: Antenna Orientation of the Access Points

Access Point	Antenna Orientation
1140 mounted on the ceiling	The Cisco logo should be pointing to the floor. Elevation: 0 degrees.
1240 mounted on the ceiling	The antenna should be perpendicular to the access point. Elevation: 0 degrees.
1240 mounted on the wall	The antenna should be parallel to the access point. Elevation: 0 degrees. If the antenna is perpendicular to the AP then the angle is 90 degrees (up or down does not matter as the dipole is omni).

Using the Automatic Hierarchy to Create Maps

Automatic Hierarchy Creation is a way for you to quickly create maps and assign access points to maps in Prime Infrastructure. You can use Automatic Hierarchy Creation to create maps, once you have added Cisco WLCs to Prime Infrastructure and named your access points. Also, you can use it after adding access points to your network to assign access points to maps in Prime Infrastructure.

Note   To use the Automatic Hierarchy Creation feature, you must have an established naming pattern for your wireless access points that provides the campus, building, floor, or outdoor area names for the maps. For example, San Jose-01-GroundFloor-AP3500i1.

To create maps using the automatic hierarchy, follow these steps:

Step 1   Choose **Design** > **Automatic Hierarchy Creation** to display the Automatic Hierarchy Creation page.

Step 2   In the text box, enter the name of an access point on your system. Or, you can choose one from the list.
This name is used to create a regular expression to create your maps.

Note   To update a previously created regular expression, select **Load and Continue** next to the expression and update the expression accordingly.

To delete a regular expression, select **Delete** next to the expression.

Step 3   Click **Next**.

Step 4   If your access point's name has a delimiter, enter it in the text box and click **Generate**. The system generates a regular expression that matches your access point's name based on the delimiter.
For example, using the dash (-) delimiter in the access point name San Jose-01-GroundFloor-AP3500i1, produces the regular expression /(.*)-(.*)-(.*)-(.*)/.

If you have a more complicated access point name, you can manually enter the regular expression.

Note   You are not required to enter the leading and trailing slashes.

Step 5   Click **Test**. The system displays the maps that will be created for the access point name and the regular expression entered.

Step 6   Using the Group fields, assign matching groups to hierarchy types.
For example, if your access point is named: SJC14-4-AP-BREAK-ROOM

In this example, the campus name is SJC, the building name is 14, the floor name is 4, and the AP name is AP-BREAK-ROOM.

Use the regular expression: /([A-Z]+)(\d+)-(\d+)-(.*)/

From the AP name, the following groups are extracted:

1   SJC

2   14

3   4

4   AP-BREAK-ROOM

The matching groups are assigned from left to right, starting at 1. To make the matching groups match the hierarchy elements, use the drop-down list for each group number to select the appropriate hierarchy element.

This enables you to have almost any ordering of locations in your access point names.

For example, if your access point is named: EastLab-Atrium2-3-San Francisco

If you use the regular expression: /(.*)-(.*)-(.*)-(.*)/ with the following group mapping:

1   Building

2   Device Name

3   Floor

4   Campus

Automatic Hierarchy Creation produces campus named San Francisco, a building under that campus named EastLab, and a floor in EastLab named 3.

Note The two hierarchy types, Not in device name and Device have no effect, but enable you to skip groups in case you need to use a matching group for some other purpose.

Automatic Hierarchy Creation requires the following groups to be mapped in order to compute a map on which to place the access point:

Table 16: Groups

Campus group present in match	Building group present in match	Floor group present in match	Resulting location
Yes	Yes	Yes	Campus > Building > Floor
Yes	Yes	No	Failed match
Yes	No	Yes	Campus > Floor (where Floor is an outdoor area)
Yes	No	No	Failed match
No	Yes	Yes	System Campus > Building > Floor
no	yes	no	failed match
no	yes	no	failed match
no	no	yes	failed match
no	no	no	failed match

Automatic Hierarchy Creation attempts to guess the floor index from the floor name. If the floor name is a number, AHC will assign the floor a positive floor index. If the floor name is a negative number or starts with the letter B (for example, b1, -4, or B2), AHC assigns the floor a negative floor index. This indicates that the floor is a basement.

When searching for an existing map on which to place the access point, AHC considers floors in the access point's building with the same floor index as the access point's name.

For example, if the map SF > MarketStreet > Sublevel1 exists and has a floor index of -1, then the access point SF-MarketStreet-b1-MON1 will be assigned to that floor."

Step 7 Click **Next**. You can test against more access points. You may test your regular expression and matching group mapping against more access points by entering the access point's names in the Add more device names to test against field, and clicking the **Add** button.
You then click the **Test** button to test each of the access points names in the table. The result of each test is displayed in the table.

If required, return to the previous step to edit the regular expression or group mapping for the current regular expression.

Step 8   Click **Next**, then click **Save** and **Apply**. This applies the regular expression to the system. The system processes all the access points that are not assigned to a map.

Note   You can edit the maps to include floor images, correct dimensions, and so on. When Automatic Hierarchy Creation creates a map, it uses the default dimensions of 20 feet by 20 feet. You will need to edit the created maps to specify the correct dimensions and other attributes. Maps created using Automatic Hierarchy Creation appear in the maps list with an incomplete icon. Once you have edited a map, the incomplete icon disappears. You may hide the column for incomplete maps by clicking the **Edit View** link.

Using the Map Editor

You use the Map Editor to define, draw, and enhance floor plan information. The map editor allows you to create obstacles so that they can be taken into consideration while computing RF prediction heatmaps for access points. You can also add coverage areas for location appliances that locate clients and tags in that particular area.

Guidelines for Using the Map Editor

Consider the following when modifying a building or floor map using the map editor:

Note   We recommend that you use the map editor to draw walls and other obstacles rather than importing a .FPE file from the legacy floor plan editor. If required, you can still import .FPE files. To do so, navigate to the desired floor area, choose **Edit Floor Area** from the Select a command drop-down list, click **Go**, select the **FPE File** check box, and browse to choose the .FPE file.

- You can add any number of walls to a floor plan with the map editor; however, the processing power and memory of a client workstation might limit the refresh and rendering aspects of the Prime Infrastructure.

Note   We recommend a practical limit of 400 walls per floor for machines with 1GB RAM or less.

- All walls are used by the Prime Infrastructure when generating RF coverage heatmaps.

Guidelines for Inclusion and Exclusion Areas on a Floor

Inclusion and exclusion areas can be of any polygon shape having at least three points.

You can only define one inclusion region on a floor. By default, an inclusion region is defined for each floor when it is added to the Prime Infrastructure. The inclusion region is indicated by a solid aqua color line, and generally outlines the region.

You can define multiple exclusion regions on a floor.

Newly defined inclusion and exclusion regions appear on heatmaps only after the Mobility Services Engine recalculates location on the floor.

Opening the Map Editor

To open the map editor, follow these steps:

Step 1 Choose **Design** > **Site Map Design**.

Step 2 Click the desired campus. The Site Maps > Campus Name page appears.

Step 3 Click a campus and then click a building.

Step 4 Click the desired floor area. The Site Maps > Campus Name > Building Name > Floor Area Name page appears.

Step 5 From the Select a command drop-down list, choose **Map Editor**, and click **Go**. The Map Editor page appears.

Using the Map Editor to Draw Coverage Areas

If you have a building that is non-rectangular or you want to mark a non-rectangular area within a floor, you can use the map editor to draw a coverage area.

To draw coverage areas using the map editor, follow these steps:

Step 1 Add the floor plan if it is not already represented in the Prime Infrastructure.

Step 2 Choose **Monitor** > **Site Maps**.

Step 3 Click the Map Name that corresponds to the outdoor area, campus, building, or floor you want to edit.

Step 4 From the Select a command drop-down list, choose **Map Editor**, and click **Go**.

Step 5 It the Map Editor page, click the **Draw Coverage Area** icon on the toolbar.
A pop-up menu appears.

Step 6 Enter the name of the area that you are defining. Click **OK**.
A drawing tool appears.

Step 7 Move the drawing tool to the area you want to outline.

- Click the left mouse button to begin and end drawing a line.

- When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page.

  The outlined area must be a closed object to appear highlighted on the map.

Step 8 Click the **disk** icon on the toolbar to save the newly drawn area.

Defining an Inclusion Region on a Floor

To define an inclusion area, follow these steps:

Step 1 Choose **Design** > **Site Maps**.

Step 2 Click the name of the appropriate floor area.

Step 3 From the Select a command drop-down list, choose **Map Editor**.

Step 4 Click **Go**.

Step 5 At the map, click the aqua box on the toolbar.

Note A message box appears reminding you that only one inclusion area can be defined at a time. Defining a new inclusion region automatically removes the previously defined inclusion region. By default, an inclusion region is defined for each floor when it is added to the Prime Infrastructure. The inclusion region is indicated by a solid aqua line and generally outlines the region.

Step 6 Click **OK** in the message box that appears. A drawing icon appears to outline the inclusion area.

Step 7 To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.

Step 8 Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.

Step 9 Repeat Defining an Inclusion Region on a Floor until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area.

Step 10 Choose **Save** from the Command menu or click the **disk** icon on the toolbar to save the inclusion region.

Note If you made an error in defining the inclusion area, click the area. The selected area is outlined by a dashed aqua line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.

Step 11 Select the **Location Regions** check box if it is not already selected. If you want it to apply to all floor maps, click **Save settings**. Close the Layers configuration page.

Step 12 To resynchronize the Prime Infrastructure and MSE databases, choose **Services** > **Synchronize Service**s.

Note If the two databases are already synchronized then a resynchronization happens automatically every time there is a change. There is no need for an explicit resynch.

Step 13 In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**. You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Note Newly defined inclusion and exclusion regions are included in location calculation only after the Mobility Services Engine recalculates location for existing devices.

Defining an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas exclusion areas in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are generally defined within the borders of an inclusion area.

To define an exclusion area, follow these steps:

Step 1   Choose **Design** > **Site Maps**.

Step 2   Click the name of the appropriate floor area.

Step 3   From the Select a command drop-down list, choose **Map Editor**.

Step 4   Click **Go**.

Step 5   On the map, click the purple box on the toolbar.

Step 6   Click **OK** in the message box that appears. A drawing icon appears to outline the exclusion area.

Step 7   To begin defining the exclusion area, move the drawing icon to a starting point on the map and click once.

Step 8   Move the drawing icon along the boundary of the area you want to exclude. Click once to start a boundary line, and click again to end the boundary line.

Step 9   Repeat Defining an Exclusion Region on a Floor until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is completely defined. The excluded area is shaded in purple.

Step 10   When all exclusion areas are defined, choose **Save** from the Command menu or click the **disk** icon on the toolbar to save the exclusion region.

> **Note**   To delete an exclusion area, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.

Step 11   Select the **Location Regions** check box if it is not already selected. If you want it to apply to all floor maps, click **Save settings**. Close the Layers configuration page when complete.

Step 12   To resynchronize the Prime Infrastructure and MSE databases, choose **Services** > **Synchronize Service**s.

> **Note**   If the two DBs are already synchronized then a resynchronization happens automatically every time there is a change. There is no need for an explicit resynch.

Step 13   In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**. You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Defining a Rail Line on a Floor

You can define a rail line on a floor that represents a conveyor belt. Additionally, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority).

> **Note**   Rail line configurations do not apply to tags.

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

To define a rail with a floor, follow these steps:

Step 1   Choose **Design** > **Site Maps**.

Step 2   Click the name of the appropriate floor area.

Step 3   Choose **Map Editor** from the Select a command drop-down list.

Step 4   Click **Go**.

Step 5   In the map, click the **rail** icon (to the right of the purple exclusion icon) on the toolbar.

Step 6   In the message dialog box that appears, enter a snap-width (feet or meters) for the rail and then click **OK**. A drawing icon appears.

Step 7   Click the **drawing** icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.

Step 8   Click the **drawing** icon twice when the rail line is completely drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.

        Note   To delete a rail line, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.

Step 9   At the floor map, choose the **Layers** drop-down list.

Step 10   Select the **Rails** check box for if it is not already selected, click **Save settings**, and close the Layers configuration panel when complete.

Step 11   To resynchronize the Prime Infrastructure and Mobility Services Engine, choose **Services** > **Synchronize Services**.

Step 12   In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**. You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Adding an Outdoor Area

Note   You can add an outdoor area to a campus map in the Prime Infrastructure database regardless of whether you have added outdoor area maps to the database.

To add an outdoor area to a campus map, follow these steps:

Step 1   If you want to add a map of the outdoor area to the database, save the map in .PNG, .JPG, .JPEG, or .GIF format. Then browse to and import the map from anywhere in your file system.

        Note   You do not need a map to add an outdoor area. You can simply define the dimensions of the area to add it to the database. The map can be any size because the Prime Infrastructure automatically resizes the map to fit the workspace.

Step 2	Choose **Design** > **Site Maps**.
Step 3	Click the desired campus to display the Design > Site Maps > Campus View page.
Step 4	From the Select a command drop-down list, choose **New Outdoor Area**.
Step 5	Click **Go**. The Create New Area page appears.
Step 6	In the New Outdoor Area page, enter the following information:

- Name—The user-defined name of the new outdoor area.

- Contact—The user-defined contact name.

- Area Type (RF Model)—Cubes And Walled Offices, Drywall Office Only, Outdoor Open Space (default).

- AP Height (feet)—Enter the height of the access point

- Image File—Name of the file containing the outdoor area map. Click **Browse** to find the file.

Step 7	Click **Next**.
Step 8	Click **Place** to put the outdoor area on the campus map. the Prime Infrastructure creates an outdoor area rectangle scaled to the size of the campus map.
Step 9	Click and drag the outdoor area rectangle to the desired position on the campus map.
Step 10	Click **Save** to save this outdoor area and its campus location to the database.
	Note A hyperlink associated with the outdoor area takes you to the corresponding Maps page.
Step 11	(Optional) To assign location presence information for the new outdoor area, choose **Edit Location Presence Info**, and click **Go**.
	Note By default, the Override Child Element Presence Info check box is selected. There is no need to alter this setting for outdoor areas.

Using Planning Mode

The planning mode opens the map editor in the browser window from which the planning tool is launched. If the original browser window has navigated away from the floor page, you need to navigate back to the floor page to launch the map editor.

You can calculate the recommended number and location of access points based on whether data and/or voice traffic and/or location are active.

Note Based on the throughput specified for each protocol (802.11a or 802.11 b/g), planning mode calculates the total number of access points required that would provide optimum coverage in your network.

Planning Mode options:

- Add APs—Enables you to add access points on a map. See the "Adding Access Points to a Floor Area" section on page 10-11 for details.

- Delete APs—Deletes the selected access points.

- Map Editor—Opens the Map Editor window.

- Synchronize with Deployment—Synchronizes your planning mode access points with the current deployment scenario.

- Generate Proposal—View a planning summary of the current access points deployment.

- Planned AP Association Tool—Allows you to add, delete, or import an AP Association from an Excel or CSV file. Once an access point is defined, it can be associated to a base radio MAC address using the Planned AP Association Tool. If the AP is not discovered, then the APs gets pushed into a standby bucket and get associated when discovered.

Note AP association is subjected to a limitation that AP should not belong to any floor or outdoor area. If the AP is already assigned to a floor or outdoor area, then the standby bucket holds the AP, and when removed from the floor or outdoor area, get positioned to the given floor. One MAC address cannot be put into a bucket for multiple floor or outdoor areas.

Note The map synchronization works only if the AP is associated to a base radio MAC address and not to its Ethernet MAC address.

Using Chokepoints to Enhance Tag Location Reporting

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be entered into the location database and plotted on the Prime Infrastructure map.

Using chokepoints in conjunction with active Cisco CX compliant tags provides immediate location information on a tag and its asset. When a Cisco CX tag moves out of the range of a chokepoint, its subsequent beacon frames do not contain any identifying chokepoint information. Location determination of the tag defaults to the standard calculation methods based on RSSIs reported by access points associated with the tag.

- Adding Chokepoints to the Prime Infrastructure, on page 90
- Adding a Chokepoint to a Prime Infrastructure Map, on page 90
- Removing Chokepoints from the Prime Infrastructure, on page 91

Adding Chokepoints to the Prime Infrastructure

To add a chokepoint to the Prime Infrastructure database, follow these steps:

Step 1   Choose **Configure** > **Chokepoints**.

Step 2   From the Select a command drop-down list, choose **Add Chokepoints**.

Step 3   Click **Go**.

Step 4   Enter the MAC address and name for the chokepoint.

Step 5   Select the **Entry/Exit Chokepoint** check box.

Step 6   Enter the coverage range for the chokepoint.

       Note   The Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 7   Click **OK**.

       Note   After the chokepoint is added to the database, it can be placed on the appropriate the Prime Infrastructure floor map.

Adding a Chokepoint to a Prime Infrastructure Map

To add the chokepoint to a map, follow these steps:

Step 1   Choose **Design** > **Site Maps**.

Step 2   In the Maps page, choose the link that corresponds to the floor location of the chokepoint.

Step 3   From the Select a command drop-down list, choose **Add Chokepoints**.

Step 4   Click **Go**.

       Note   The Add Chokepoints summary page lists all recently added chokepoints that are in the database but are not yet mapped.

Step 5   Select the check box next to the chokepoint that you want to place on the map.

Step 6   Click **OK**.

A map appears with a chokepoint icon located in the top left-hand corner. You are now ready to place the chokepoint on the map.

Step 7   Left-click the chokepoint icon and drag it to the proper location.

       Note   The MAC address, name, and coverage range of the chokepoint appear in the dialog box in the left when you click the chokepoint icon for placement.

Step 8   Click **Save**.

The floor map page reappears and the added chokepoint appears on the map.

       Note   The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.

Note   The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

Note   The MAC address, name, entry or exit chokepoint, static IP address, and range of the chokepoint appear when you hover your mouse cursor over its map icon.

Step 9   If the chokepoint does not appear on the map, select the **Chokepoints** check box located in the Floor Settings menu.

Note   Do not click **Save Settings** unless you want to save this display criteria for all maps.

Note   You must synchronize network design to the Mobility Services Engine or location server to push chokepoint information.

Removing Chokepoints from the Prime Infrastructure

You can remove one or more chokepoints at a time. To delete a chokepoint, follow these steps:

Step 1   Choose **Configure** > **Chokepoints**. The Chokepoints page appears.

Step 2   Select the check box next to the chokepoint to be deleted.

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

Step 4   To confirm the chokepoint deletion, click **OK** in the dialog box that appears.
The Chokepoints page reappears and confirms the deletion of the chokepoints. The deleted chokepoints are no longer listed in the page.

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:

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:

Guidelines and Limitations

- The Mobility Services Engine (MSE) can only be configured from one Prime Infrastructure.

- If your wIPS deployment consists of a controller, access point, and MSE, you must set the controller and MSE to UTC timezone.

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

Prerequisites

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). See the *Cisco 3350 Mobility Services Engine Getting Started Guide* or *Cisco 3310 Mobility Services Engine Getting Started Guide.*

2 Add the Mobility Services Engine to the Prime Infrastructure (if not already added).

3 Configure access points to operate in wIPS monitor mode or Local wIPS mode.

4 Configure wIPS profiles.

Information About wIPS Configuration and Profile Management

Configuration of wIPS profiles follows a chained hierarchy starting with Prime Infrastructure, which is used for profile viewing and modification. The actual profiles are stored within the wIPS service running on the 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.

When a configuration change to a wIPS profile is made at Prime Infrastructure and applied to a set of Mobility Services Engines and controllers, the following occurs:

1 The configuration profile is modified on Prime Infrastructure 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.

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.

This section contains the following topics:

Guidelines and Limitations

- Only Cisco Aironet 1130, 1140, 1240, 1250, 1260, 1600, 2600, 3600, 3502E, and 3502I Series Access Points support wIPS monitor mode.

Configuring Access Points for wIPS Monitor Mode

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

Step 1   Choose **Configure > Access Points**.

Step 2   Click the **802.11a** or **802.11b/g** radio link.

Figure 11: Configure > Access Points > Radio

Step 3   In the Access Point page, uncheck the **Admin Status** check box to disable the radio.

Figure 12: Access Points > Radio

Step 4   Click **Save**.

Note   Repeat these steps for each radio on an access point that is to be configured for wIPS monitor mode.

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

Step 6 In the access point dialog box, choose **Monitor** from the AP Mode drop-down list.

Figure 13: Configure > Access Points > Access Point Detail

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

Step 8 From the Monitor Mode Optimization drop-down list, choose **WIPS**.
This will place the AP radios and the module radio in monitor mode.

If you want to place the AP radios in ELM mode and the module radio in monitor mode, you have to select local for AP mode and submide as wIPS.

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 the appropriate access point radio.

Figure 14: Configure > Access Points > Radio

Step 13 In the Radio Detail page, select the Admin Status **Enabled** check box.

Step 14 Click **Save**.
Repeat this procedure 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 the Prime Infrastructure. This profile is pre-tuned with a majority of attack alarms enabled by default, and monitors attacks against access points within the same RFGroup as the wIPS access points. In this manner, the system is 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 following configuration steps that follow are marked as Overlay-Only and are only to be undertaken when deploying the 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 Choose **Configure** > **wIPS Profiles**.
The wIPS Profiles page appears.

Step 2 From the Select a command drop-down list, choose **Add Profile** and click **Go**.

Step 3 **Selecting a Profile Template**
In the Profile Parameters dialog box, choose a profile template from the Copy From drop-down list.

Note The wIPS comes with a pre-defined set of profile templates from which you can select or use as a basis for custom profiles. Each profile is tailored to either a specific business or application as are the specific alarms enabled on that profile.
Note You cannot edit the default profile.
Note Ensure that the NMSP session is active to push the profile to the controller.

Figure 15: Profile Parameters Dialog Box
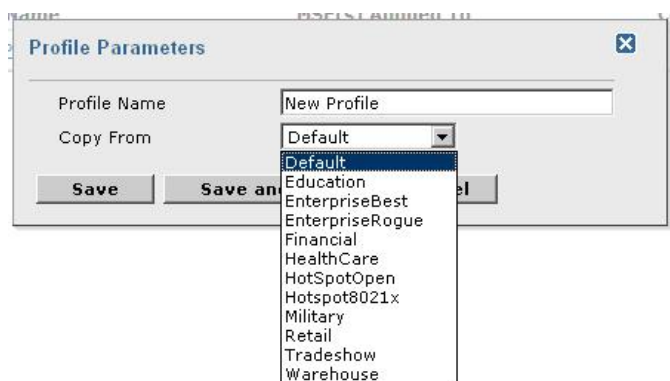
Step 4 After selecting a profile and entering a profile name, click **Save and Edit**. Fore more information, see the wIPS Profiles, on page 103 section.

Step 5 **Configure the SSIDs to Monitor**

(Optional) Configure SSIDs in the SSID Group List page. By default, a 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 16: SSID Groups Summary Pane

1   Select the **MyWLAN** check box and choose **Edit Group** from the drop-down list, then click **Go**.

2   Enter SSIDs to Monitor. This step is required if the system to be utilized to monitor attacks against a different WLAN infrastructure is typical of an overlay deployment model.

3   Enter the SSID name (separate multiple entries by a single space) and click **Save**.

The SSID Groups page appears confirming that the SSIDs are added successfully. For more information, see the Configuring wIPS SSID Group List, on page 106 section.

Figure 17: New Profile > SSID Groups Page

4   Click **Next**.

The Select Policy and Policy Rules summary panes appear.

Figure 18: Next > Select Policy Summary Pane
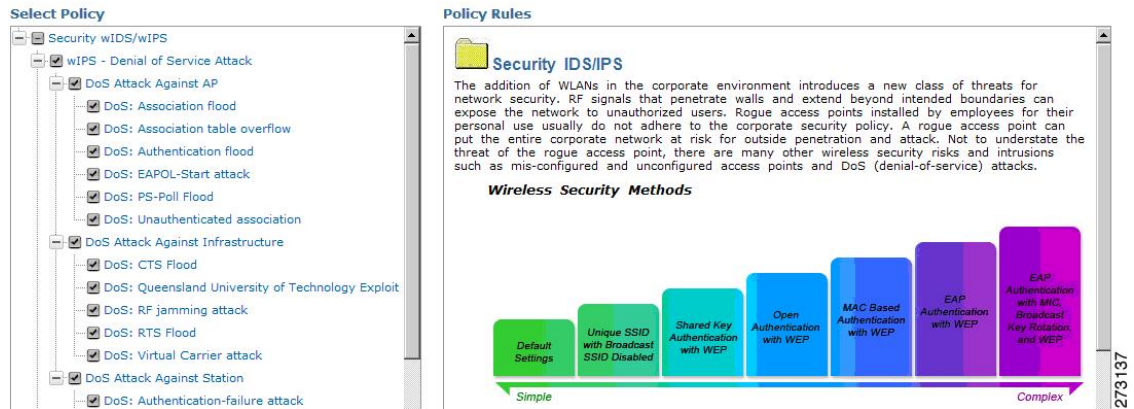
Step 6   `Editing the Profile`
To enable or disable attacks to be detected and reported, select the check box next to the specific attack type in question in the Select Policy pane.

Step 7   To edit the profile, click the name of the attack type (such as DoS: Association flood).
The configuration pane for that attack type appears in the right pane above the policy rule description.

Figure 19: Policy Rules Pane

Step 8   `Editing the Policy Rules`.
To modify a policy rule, select the check box next to the policy rule in the Policy Rules page and click **Edit**.

The Policy Rule Configuration dialog box appears. Configure the following in the **Policy Rule Configuration** dialog box:

Figure 20: Policy Rule Configuration Dialog Box

a) Choose the severity of the alarm to be modified from the **Severity** drop-down list. The possible options are **Minor**, **Major**, **Critical**, and **Warning**.

b) Select the **Containment** check box to enable the auto containment action.

   Note The following security penetration attacks can be configured for Rogue AP containment in Release 7.5:

   • Soft AP or Host AP Detected

   • Airsnarf Attack Detected

   • Honeypot AP Detected

   • Hotspotter Tool Detected

   • Karma Tool Detected

   • Device Broadcast XSS SSID

c) Select 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 monitors for attacks from the **SSID Group** drop-down list.

   • If you select SSID, continue with Step 9.

   • If you select Device Group, continue with Step 10.

   Note The default types are Device Group and Internal. . 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 9 Add Policy Rules (Optional)
(Optional), For overlay deployments only, to add a policy rule for an SSID, do the following steps:

1 To add a policy rule, click **Add**.

Figure 21: Adding a Policy Rule

2 In the **Policy Rule Configuration** dialog box, choose **MyWLAN** from the SSID Group list.

> **Note** SSID is already selected as the type.

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

4 Modify each policy rule. Continue with Step 10 when all modifications 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. You must create a policy rule under each separate alarm that defines the system to monitor attacks against the SSID Group created earlier.

Figure 22: Edit Policy Rules for SSID Monitoring
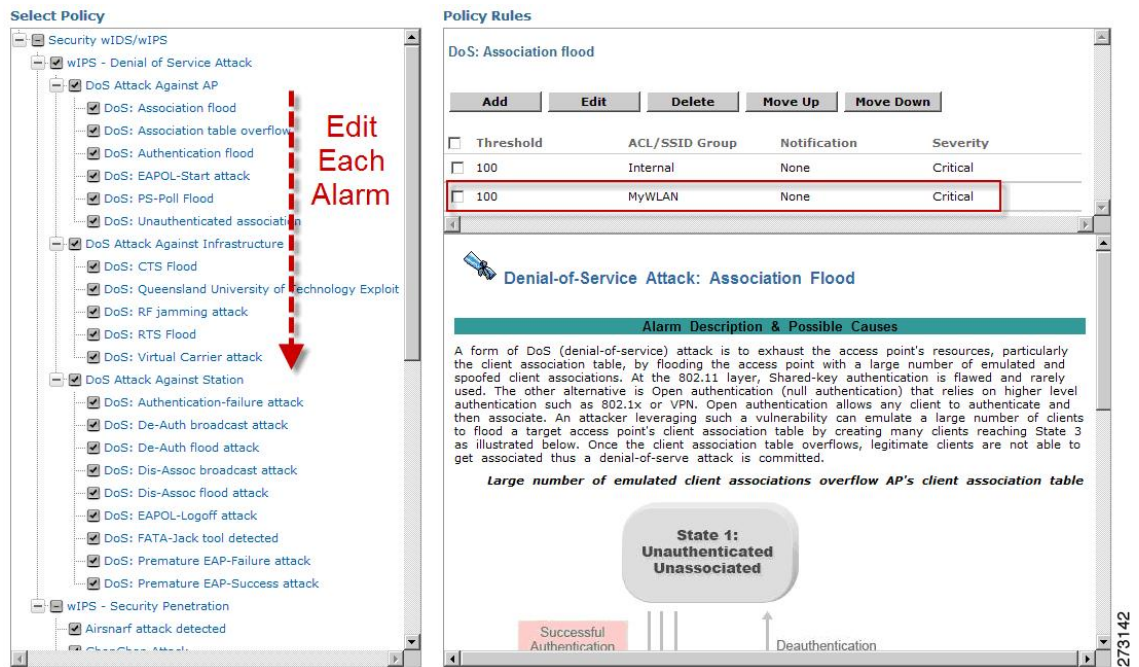
Step 10 In the Profile Configuration dialog box, click **Save** to save the Profile (SSID or Device Group) and then click **Next**.

Figure 23: Profile Configuration Dialog box

WIPS Profiles > Profile > 'New Profile' > Profile Configuration

```
[ Save ]   [ Cancel ]   [ Back ]   [ Next ]
```
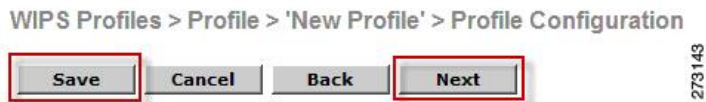
Step 11 Select the MSE/Controller combinations to apply the profile to and then click **Apply**.

Figure 24: Apply Profile Dialog Box

WIPS Profiles > Profile > 'New Profile' > Apply Profile

```
[ Apply ]   [ Cancel ]   [ Back ]
```

Select MSE/Controller(s)

- ☑ MSE/Controller(s)
  - ☑ MSE-1
    - ☑ WLC-1
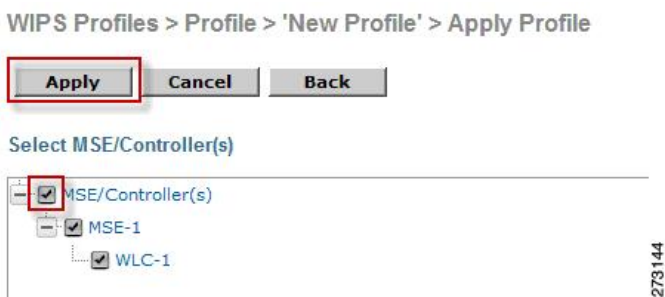
wIPS Profiles

The wIPS Profiles > Profile List page allows you to view, edit, apply, or delete current wIPS profiles and to add new profiles.

Tip To learn more about Cisco Adaptive wIPS features and functionality, go to http://www.cisco.com/en/US/products/ps9817/index.html

To access the wIPS profile list for the Prime Infrastructure, choose **Configure > wIPS Profiles**. The page displays wIPS Profiles > Profile List. If the Profile List is not currently displayed, choose **Profile List** from the left sidebar menu of wIPS profiles.

The Profile List provides the following information for each profile:

- Profile Name—Indicates the user-defined name for the current profile. Click the profile name to view or edit profile details.

  Note When you hover your mouse over the profile name, the Profile ID and version appear.

- MSE(s) Applied To—Indicates the number of Mobility Services Engines (MSEs) to which this profile is applied. Click the MSE number to view profile assignment details.

- Controller(s) Applied To—Indicates the number of controllers to which this profile is applied. Click the controller number to view profile assignment details.

This section contains the following topics:

- Adding a Profile

- Deleting a Profile

- Applying a Current Profile

The profile editor allows you to create new profiles or modify current profiles. See the Profile Configuration Using the Profile Editor for more information.

Adding a Profile

A new wIPS profile can be created using the default or pre-configured profile.

Tip To learn more about Cisco Adaptive wIPS features and functionality, go to Cisco.com to watch a multimedia presentation. Here you will also find learning modules for a variety of the Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

To add a wIPS profile, follow these steps:

Step 1 Select **Configure > wIPS Profiles**. The page displays the wIPS Profiles > Profile List.

Step 2 From the Select a command drop-down list, choose **Add Profile**.

Step 3 Click **Go**.

Step 4 Type a profile name in the Profile Name text box of the Profile Parameters page.

Step 5 Select the applicable pre-defined profile, or choose **Default** from the drop-down list. Pre-defined profiles include the following:

- Education

- EnterpriseBest

- EnterpriseRogue

- Financial

- HealthCare

- HotSpotOpen

- Hotspot8021x

- Military

- Retail

- Tradeshow

- Warehouse

Step 6 Select one of the following:

- Save—Saves the profiles to the Prime Infrastructure database with no changes and no Mobility Services Engine or controller assignments. The profile appears in the profile list.

- Save and Edit—Saves the profile and allows you to edit the profile.

- Cancel—Closes the Profile Parameters page without creating a profile.

Deleting a Profile

To delete a wIPS profile, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List.

Step 2 Select the check box of the wIPS profile(s) you want to delete.

Step 3 From the Select a command drop-down list, choose **Delete Profile**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Note   If the profile is already applied to a controller, it cannot be deleted.

Applying a Current Profile

🔎

Tip   To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http:// www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html. Here you will also find learning modules for a variety of the Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

You cannot apply wIPS profile to WLC 7.5 and earlier release using PI 1.4.x or PI 2.x with MSE 7.6 release.

To apply a wIPS profile, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List.

Step 2 Select the check box of the wIPS profile(s) you want to apply.

Step 3 From the Select a command drop-down list, choose **Apply Profile**.

Step 4 Click **Go**.

Step 5 Select the Mobility Services Engine(s) and controller(s) to which the profile is applied.

Note   If the new assignment is different than the current assignment, you are prompted to save the profile with a different name

Step 6   When applicable Mobility Services Engine(s) and controller(s) are selected, choose one of the following:

- Apply—Applies the current profile to the selected Mobility Services Engine/controller(s).

- Cancel—Returns to the profile list with no changes made.

Configuring wIPS SSID Group List

The SSID (Service Set IDentifier) is a token or key which identifies an 802.11 (Wi-Fi) network. You must know the SSID to join an 802.11 network. SSIDs can be associated with a wIPS profile as a group by using the SSID group list feature.

An SSID group can be added to a profile by importing it from the Global SSID Group List page (Configure > wIPS Profiles > SSID Group List) or by adding one directly from the SSID Groups page.

This section contains the following topics:

- Global SSID Group List

- SSID Groups

φ

Tip   Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.htmlHere you will also find learning modules for a variety of Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

Global SSID Group List

The SSID Group List page allows you to add or configure global SSID groups that you might later import into an applicable wIPS profile.

φ

Tip   To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.htmlHere you will also find learning modules for a variety of the Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

To access the SSID Group List page, choose **Configure > wIPS Profiles**. From the left sidebar menu, choose **SSID Group List**. The SSID Group List page displays the current SSID groups and their associated SSIDs.

This section contains the following topics:

- Adding a Group

- Editing a Group

- Deleting a Group

Adding a Group

To add an SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **SSID Group List**.

Step 3 From the Select a command drop-down list, choose **Add Group**.

Step 4 Click **Go**.

Step 5 On the SSID configuration page, type an SSID group name in the available text box.

Step 6 Enter the SSIDs in the SSID List text box. Separate multiple SSIDs with a space.

Step 7 When finished, select one of the following:

- Save—Saves the SSID group and adds it to the SSID Group List.

- Cancel—Closes the SSID configuration page without saving the new SSID group.

  Note   To import the SSID groups to a profile, choose **Configure > wIPS Profile**. Click the applicable profile name to open to open the SSID Groups page. From the Select a command drop-down list, choose **Add Groups from Global List**. Select the check box(es) for the SSID group(s) you want to import and click **Save**.

Editing a Group

To edit a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **SSID Group List**.

Step 3 Select the check box of the SSID group that you want to edit.

Step 4 From the Select a command drop-down list, choose **Edit Group**.

Step 5 Click **Go**.

Step 6 In the SSID configuration page, make the necessary changes to the SSID group name or SSID list.

Step 7 When finished, select one of the following:

- Save—Saves the current changes and closes the SSID configuration page.

- Cancel—Closes the SSID configuration page without saving the changes.

Deleting a Group

To delete a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **SSID Group List**.

Step 3 Select the check box of the SSID group(s) that you want to delete.

Step 4 From the Select a command drop-down list, choose **Delete Group**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion.

SSID Groups

The SSID Groups page is the first page displayed when you access the profile editor. This page displays SSID groups that are included for the current wIPS profile.

From this page, you can add, import, edit, or delete an SSID group for the current profile.

Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html. Here you also find learning modules for a variety of the Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

This section contains the following topics:

- Adding a Group
- Adding Groups from Your Global List
- Editing a Group
- Deleting Group

Adding a Group

To add an SSID Group to the current wIPS profile, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **Profile List**.

Step 3 Click the profile name of the applicable wIPS profile.

Step 4 From the Select a command drop-down list, choose **Add Group**.

Step 5 Click **Go**.

Step 6 On the SSID configuration page, type an SSID group name in the available text box.

Step 7 Enter the SSIDs in the SSID List text box. Separate multiple SSIDs with commas.

Step 8 When finished, select one of the following:

• Save—Saves the SSID group and adds it to the SSID Group List.

• Cancel—Closes the SSID configuration page without saving the new SSID group.

Adding Groups from Your Global List

SSID groups can also be added by importing them from your Global SSID Groups list. See the Global SSID Group List for more information on creating a global SSID groups list.

To import SSID groups into a profile, follow these steps:

Step 1   Select **Configure > wIPS Profile**.

Step 2   Click the profile name for the applicable profile to open the SSID Groups page.

Step 3   From the Select a command drop-down list, choose **Add Groups from Global List**.

Step 4   Select the check box(es) for the SSID group(s) you want to import.

Step 5   Click **Save**.

Editing a Group

To edit a current SSID Group, follow these steps:

Step 1   Choose **Configure > wIPS Profiles**.

Step 2   From the left sidebar menu, choose **Profile List**.

Step 3   Click the applicable wIPS profile names.

Step 4   Select the check box of the SSID group that you want to edit.

Step 5   From the Select a command drop-down list, choose **Edit Group**.

Step 6   Click **Go**.

Step 7   In the SSID configuration page, make the necessary changes to the SSID group name or the SSID list.

Step 8   When finished, select one of the following:

• Save—Saves the current changes and closes the SSID configuration page.

• Cancel—Closes the SSID configuration page without saving the changes.

Deleting Group

To delete a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **Profile List**.

Step 3 Click the profile name of the applicable wIPS profile.

Step 4 Select the check box of the SSID group that you want to delete.

Step 5 From the Select a command drop-down list, choose **Delete Group**.

Step 6 Click **Go**.

Step 7 Click **OK** to confirm the deletion.

Profile Configuration Using the Profile Editor

Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html. Here you also find learning modules for a variety of the Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

The profile editor allows you to configure profile details including the following:

- SSID groups—Add, edit, or delete SSID groups.

- Policy inclusion—Determines the policies that are included in the profile.

- Policy level settings—Configure settings for each policy such as threshold, severity, notification type, and ACL/SSID groups.

- MSE/controller applications—Select the Mobility Services Engine(s) or controller(s) to which you want to apply the profile.

To configure profile details, follow these steps:

Step 1 Access the profile editor. This can be done in two ways:

- When creating a new profile, click **Save and Edit** in the Profile Parameters page.

- Click the profile name from the Profile List page.

Step 2 From the SSID Groups page, you can edit and delete current groups or add a new group. For more information on adding, editing, or deleting SSID groups, see the Configuring wIPS SSID Group List for more information.

Step 3 When SSID groups have been added or edited as needed, select one of the following:

- Save—Saves the changes made to the SSID groups.

　　　　• Cancel—Returns to the profile list with no changes made.

　　　　• Next—Proceeds to the Profile Configuration page.

Step 4　From the Profile Configuration page, you can determine which policies are included in the current profile. The check boxes in the policy tree (located in the left Select Policy pane) indicate which policies are enabled or disabled in the current profile. You can enable or disable an entire branch or individual policy as needed by selecting the check box for the applicable branch or policy.

Note　By default, all policies are selected.

Note　For detailed information regarding each of the wIPS policies, see the wIPS Policy Alarm Encyclopedia.

Step 5　In the Profile Configuration page, click an individual policy to display the policy description and view or modify current policy rule settings.

The following options are available for each policy:

　　　　• Add—Click **Add** to access the Policy Rule Configuration page to create a new rule for this policy.

　　　　• Edit—Select the check box of the applicable rule, and click **Edit** to access the Policy Rule Configuration page to edit the settings for this rule.

　　　　• Delete—Select the check box of the rule you want to delete and click **Delete**. Click **OK** to confirm the deletion.

　　　　Note　There must be at least one policy rule in place. You cannot delete a policy rule if it is the only one in the list.

　　　　• Move Up—Select the check box of the rule you want to move up in the list and click **Move Up**.

　　　　• Move Down—Select the check box of the rule you want to move down in the list and click **Move Down**.

　　　　The following settings can be configured at the policy level:

　　　　• Threshold (not applicable to all policies)—Indicates the threshold or upper limit associated with the selected policy. When the threshold is reached for a policy, an alarm is triggered.

　　　　Note　Because every policy must contain at least one threshold, default thresholds are defined for each depending on the standard wireless network issues.

　　　　Note　Threshold options vary based on the selected policy.

　　　　Note　Alarms from Cisco Adaptive wIPS DoS and security penetration attacks are classified as security alarms. A summary of these attacks is located in the Security Summary page. Choose **Monitor > Security** to access this page. The wIPS attacks are located in the Threats and Attacks section.

　　　　• Severity—Indicates the level of severity of the selected policy. Parameters include critical, major, info, and warning. The value of this field might vary depending on the wireless network.

　　　　• Notification—Indicates the type of notification associated with the threshold.

　　　　• ACL/SSID Group—Indicates the ACL or SSID Group(s) to which this threshold is applied.

　　　　Note　Only selected groups trigger the policy.

Step 6　When the profile configuration is complete, select one of the following:

　　　　• Save—Saves the changes made to the current profile.

- Cancel—Returns to the profile list with no changes made.

- Back—Returns to the SSID Groups page.

- Next—Proceeds to the MSE/Controller(s) page.

Step 7   In the Apply Profile page, select the check box(es) of the Mobility Services Engine and controller(s) to which you want to apply the current profile.

Step 8   When the applicable Mobility Services Engine(s) and controller(s) are selected, choose one of the following:

- Apply—Applies the current profile to the selected Mobility Services Engine/controller(s).

- Cancel—Returns to the profile list with no changes made.

Note   A created profile can also be applied directly from the profile list. From the Profile List page, select the check box of the profile you want to apply and click **Apply Profile** from the Select a command drop-down list. Click **Go** to access the Apply Profile page.

C H A P T E R 7

Monitoring the System and Services

This chapter describes how to monitor the Cisco Mobility Services Engine by configuring and viewing alarms, events, and logs and how to generate reports on system use and element counts (tags, clients, rogue clients, interferers, and access points). This chapter also describes how to use the Prime Infrastructure to monitor clients (wired and wireless), tags, chokepoints, and Wi-Fi TDOA receivers.

- Working with Alarms, page 113
- Working with Events, page 119
- Working with Logs, page 119
- Monitoring Access Points Details, page 121
- Generating Reports, page 136
- Creating a Device Utilization Report, page 140
- Client Support on the MSE, page 143
- Monitoring Geo-Location, page 150
- Ekahau Site Survey Integration, page 151
- AirMagnet Survey and Planner Integration, page 152
- Interpreting Security Dashboard, page 152

Working with Alarms

This section describes how to view, assign, and clear alarms on a Mobility Services Engine using the Prime Infrastructure. It also describes how to define alarm notifications (all, critical, major, minor, warning) and how to e-mail those alarm notifications.

- Guidelines and Limitations, on page 114
- Viewing Alarms, on page 114
- Monitoring Cisco Adaptive wIPS Alarm Details, on page 115
- Assigning and Unassigning Alarms, on page 117
- Deleting and Clearing Alarms, on page 118

• E-mailing Alarm Notifications, on page 118

Guidelines and Limitations

Once the severity is cleared, the alarm is deleted from the Prime Infrastructure after 30 days.

Viewing Alarms

To view Mobility Services Engine alarms, follow these steps:

Step 1   Choose **Monitor** > **Alarms**.

Step 2   Click the **Advanced Search** link in the navigation bar. A configurable search dialog box for alarms appears.

Step 3   Choose **Alarms** from the Search Category drop-down list.

Step 4   Choose the severity of alarms from the Severity drop-down list. The options are All Severities, Critical, Major, Minor, Warning, or Clear.

Step 5   Choose **Mobility Service** from the Alarm Category drop-down list.

Step 6   Choose the **Condition** from the Condition combo box. Alternatively, you can enter the condition in the Condition text box.

Step 7   From the Time Period drop-down list, choose the time frame for which you want to review alarms.
The options range from minutes (5, 15, and 30) to hours (1 and 8) to days (1 and 7). To display all, choose **Any time**.

Step 8   Select the **Acknowledged State** check box to exclude the acknowledged alarms and their count in the Alarm Summary page.

Step 9   Select the **Assigned Stat**e check box to exclude the assigned alarms and their count in the Alarm Summary page.

Step 10   From the Items per page drop-down list, choose the number of alarms to display in each page.

Step 11   To save the search criteria for later use, select the **Save Search** check box and enter a name for the search.
   Note   You can initiate the search thereafter by clicking the **Saved Search** link.

Step 12   Click **Go**. The alarms summary dialog box appears with search results.
   Note   Click the column headings (Severity, Failure Source, Owner, Date/Time, Message, and Acknowledged) to sort alarms.

Step 13   Repeat Step 2 to Step 12 to see Context-Aware Service notifications for the Mobility Services Engine. Enter Context Aware Notifications as the alarm category in Step 5.

wIPS Alarm Consolidation

The wIPS alarm consolidation feature is introduced in Release 7.5. The wIPS alarm consolidation aggregates different wireless intrusion incidents reported by access points and provides a concise meaningful alarm. This helps you to quickly separate the potential security issues and concerns. Alarm consolidation is performed at wIPS services module in the MSE. After the consolidation rule is triggered in MSE, the MSE notifies the Prime Infrastructure by sending an SNMP trap.

The following three attack consolidation categories are created:

- Beacon flood—The system detects a number of out of sequence beacon frames sent from a device. By sending fake beacon frames, the hacker can advertise false access point configuration and settings such as supported data rate, SSID, and channel information. The following alarms are included in this alarm consolidation category:

  ○ Spoofed MAC Address Detected

  ○ DoS: Beacon Flood

- De-auth flood—This is a type of denial-of-service attack. The traffic pattern matches with the denial-of-service attack that uses spoofed de-authentication frames to break the association between an access point and its client stations.

  The following alarms are included in this alarm consolidation category:

  ○ Spoofed MAC address

  ○ DoS: De-Auth Flood

- MDK3-Destruction attack—This causes all clients that is associated or trying to associate with the AP to fail. The following alarms are included in this consolidation category:

  ○ DoS: De-Auth Broadcast Flood

  ○ DoS: Dis-Assoc Broadcast Flood

  ○ DoS: Unauthenticated Association

  ○ Dos: MDK3-Destruction Attack

Monitoring Cisco Adaptive wIPS Alarm Details

To view MSE alarm details, follow these steps:

Choose **Monitor** > **Alarms** > *failure object* to view details of the selected Cisco wIPS alarm. The following alarm details are provided for Cisco Adaptive wIPS alarms:

- General Properties—The general information might vary depending on the type of alarm. For example, some alarm details might include location and switch port tracing information. The following table describes the general parameters associated with the MSE Alarm and wIPS Traps condition.

  ○ Detected By wIPS AP—The access point that detected the alarm.

  ○ wIPS AP IP Address—The IP address of the wIPS access point.

  ○ Owner—Name of person to which this alarm is assigned or left blank.

  ○ Acknowledged—Displays whether or not the alarm is acknowledged by the user.

  ○ Category—For wIPS, the alarm category is Security.

  ○ Created—Month, day, year, hour, minute, second, AM or PM that the alarm was created.

◦ Modified—Month, day, year, hout, minute, second, AM or PM that the alarm was last modified.

◦ Generated By—Indicates how the alarm event was generated (either NMS or from a trap).

NMS (Network Management System - Prime Infrastructure—Generated through polling. Prime Infrastructure periodically polls the Cisco WLCs and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events. in this case, "Generated by" NMS.

Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them. In this case, "Generated by" is controller.

◦ Severity—Level of severity including critical, major, minor, warning, and clear.

◦ Last Disappeared—The date and time that the potential attack last disappeared.

◦ Channel—The channel on which the potential attack occurred.

◦ Attacker Client/AP MAC—The MAC address of the client or access point that initiated the attack.

◦ Attacker Client/AP IP Address—The IP address of the client or access point that initiated the attack.

◦ Target Client/AP IP Address—The IP address of the client or access point targeted by the attacker.

◦ Controller IP Address—The IP address of the controller to which the access point is associated.

◦ MSE—The IP address of the associated Mobility Services Engine.

◦ Controller MAC address—The MAC address of the controller to which the access point is associated.

◦ wIPS access point MAC address

◦ Forensic File

◦ Event History—Takes you to the Monitoring Alarms page to view all events for this alarm.

• Annotations—Enter any new notes in this text box and click **Add** to update the alarm. Notes appear in the "Annotations" display area.

• Messages—Displays the alarm name.

• Description—Displays the consolidated information about the alarm.

• Mitigation Status—Displays what mitigation action was initiated against the attack.

• Audit Report—Click to view config audit alarm details. This report is only available for Config Audit alarms.

Configuration audit alarms are generated when audit discrepancies are enforced on config groups.

Note If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group. The alarms have links to the audit report where you can view a list of discrepancies for each controller.

- Event History—Opens the MSE Alarm Events page to view events for this alarm. When there are multiple alarm pages, the page numbers appear at the top of the page with a scroll arrow on each side. Use these scroll arrows to view additional alarms.

- Rogue Clients—If the failure object is a rogue access point, information about rogue clients is displayed.

- Map Location—Displays the map location for the alarm.

  ◦ Floor—The location where this attack was detected.

  ◦ Last Located At—The last time where the attack was located.

  ◦ On MSE—The mobility server engine in which this attack was located.

  ◦ Location History—Click the Location History to see details on the current attacker and victim location.

Note Out of all the alarms reported by wIPS, the following four alarms are detected at the wIPS server in the Mobility Services Engine (MSE) and not in the access point. For these alarms, currently there is no location information present. The list of alarms are:

- 124 Hotspotter tool detected

- 133 Day-Zero attack by device security anomaly

- 135 Day-Zero attack by WLAN security anomaly

- 138 Unauthorized association by vendor list

- Related Alarm List—Lists all the alarms related to a particular attack. This shows what consolidation rule was used to consolidate the alarms.

  ◦ Alarm Name—Name of the alarm.

  ◦ First Heard—Indicates the date and time when the attack first seen.

  ◦ Last Heard—Indicates the date and time when the attack was last seen.

  ◦ Status—Status of the attack.

Assigning and Unassigning Alarms

To assign and unassign an alarms, follow these steps:

Step 1 Choose **Monitors** > **Alarms** to display the Alarms page.

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

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

Step 3 Choose **Assign > Assign to Me (or Unassign)**.

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, the Prime Infrastructure removes it from its database. If you clear an alarm, it remains in the Prime Infrastructure 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   Choose **Monitors** > **Alarms** to display the Alarms page.

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

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

E-mailing Alarm Notifications

The Prime Infrastructure lets you send alarm notifications to a specific e-mail address. Sending notifications through e-mail enables you to take prompt action when needed.

You can choose the alarm severity types (critical, major, minor, and warning) to have e-mailed to you.

To send alarm notifications to e-mail, follow these steps:

Step 1   Choose **Monitor > Alarms**.

Step 2   Select the alarms by selecting their corresponding check boxes. Click **Email Notification** . The Email Notification page appears.
    Note   An SMTP mail server must be defined before you enter target e-mail addresses for e-mail notification. Choose **Administration > Settings > Mail Server Configuration** to enter the appropriate information.

Step 3   Select the **Enabled** check box next to the Mobility Service.
    Note   Enabling the **Mobility Service** alarm category sends all alarms related to Mobility Services Engine and the location appliance to the defined e-mail address.

Step 4   Click the **Mobility Service** link. The page for configuring the alarm severity types that are reported for the Mobility Services Engine appears.

Step 5   Select the check box next to all the alarm severity types for which you want e-mail notifications sent.

Step 6   In the **To** text box, enter the e-mail address or addresses to which you want the e-mail notifications sent. Separate e-mail addresses by commas.

Step 7   Click **OK**.
You are returned to the Alarms > Notification page. The changes to the reported alarm severity levels and the recipient e-mail address for e-mail notifications are displayed.

Working with Events

You can use Prime Infrastructure to view the Mobility Services Engine and location notification events. You can search and display events based on their severity (critical, major, minor, warning, clear, and info) and their category.

This section contains Displaying Location Notification Events procedure.

Displaying Location Notification Events

To display location notification events, follow these steps:

Step 1   Choose **Monitor > Events**.

Step 2   In the Events page, you can perform the following:

- 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 text box of the navigation bar. Click **Search**.

- To display events by severity and category, click **Advanced Search** in the navigation bar and choose the appropriate options from the Severity and Event Category drop-down lists box. Click **Go**.

Step 3   If Prime Infrastructure finds events that match the search criteria, it shows a list of these events.

Note   For more information about an event, click the failure source 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.

Guidelines and Limitations

- When you are selecting an appropriate option from the logging level, make sure you use Error and Trace only when directed to do so by Cisco TAC personnel.

- Enable advanced debugging only under the guidance of Cisco TAC personnel because advanced debugging slows the mobility service down.

Configuring Logging Options

You can use Prime Infrastructure to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

Step 1   Choose **Services > Mobility Services Engines**.

Step 2   Click the name of the MSE that you want to configure.

Step 3   From the System menu, choose **Logs**. The logging options for the selected MSE appear.

Step 4   Choose the appropriate options from the Logging Level drop-down list.
There are four logging options: **Off**, **Error**, **Information**, and **Trace**.

All log records with a log level of **Error** or above are logged to a new error log file locserver-error-%u-%g.log. This is an additional log file maintained along with the location server locserver-%u-%g.log log file. The error log file consists of logs of **Error** level along with their context information. The contextual information consists of 25 log records prior to the error. You can maintain up to 10 error log files. The maximum size allowed for each log file is 10 MB.

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

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

Step 6   Select the **Enable** check box under Advanced Parameters to enable advanced debugging. By default, this option is disabled.
> **Caution**   Enable advanced debugging only under the guidance of Cisco TAC personnel because advanced debugging slows the mobility service down.

Step 7   To download log files from the server, click **Download Logs**. For more information, see the Downloading Log Files.

Step 8   In the Log File group box, enter the following:

- The number of log files to be maintained in the MSE. You can maintain a minimum of 5 log files and a maximum of 20 log files in the MSE.

- The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.

Step 9   In the MAC Address Based Logging page, do the following:

- Select the **Enable** check box to enable MAC address logging. By default, this option is disabled.

- Add one or more MAC addresses for which you want to enable logging. You can also remove MAC addresses that you have already added by selecting the MAC address from the list and clicking **Remove**.

  For more information on MAC-address-based logging, see the MAC address-based Logging.

Step 10   Click **Save** to apply your changes.

MAC address-based Logging

This feature allows you to create log files that are specific to an entity whose MAC address is specified. The log files are created in the locserver directory under the following path:

```
/opt/mse/logs/locserver
```
A maximum of 5 MAC addresses can be logged at a time. The log file format for MAC address aa:bb:cc:dd:ee:ff is:

macaddress-debug-aa-bb-cc-dd-ee-ff.log

You can create a maximum of two log files for a MAC address. The two log files may consist of one main and one back up or rollover log file.

The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC address. The MAC log files which are not updated for more than 24 hours are pruned.

Downloading Log Files

If you need to analyze Mobility Services Engine log files, you can use Prime Infrastructure to download them to your system. The Prime Infrastructure downloads a .zip file containing the log files.

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

Step 1   Choose **Services > Mobility Services**.

Step 2   Click the name of the Mobility Services Engine to view its status.

Step 3   From the left sidebar menu, choose **Logs**.

Step 4   Click **Download Logs**.

Step 5   Follow the instructions in the File Download dialog box to view the file or save the .zip file to your system.

Monitoring Access Points Details

The Access Points Details page enables you to view access point information for a single AP.

Choose **Monitor > Access Points** and click an item in the AP Name column to access this page. Depending on the type of access point, the following tabs might be displayed. This section provides the detailed information regarding each Access Points Details page tab and contains the following topics:

- General Tab
- Interfaces Tab
- CDP Neighbors Tab
- Current Associated Clients Tab
- SSID Tab
- Clients Over Time Tab

General Tab

✎

Note The General tab fields differ between lightweight and autonomous access points.

This section contains the following topics:

- General—Lightweight Access Points
- General—Autonomous

General—Lightweight Access Points

Table 5-47 lists the General (for Lightweight Access Points) Tab fields.

Table 17: General (for Lightweight Access Points) Tab Fields

Field	Description
General	
AP Name	Operator defined name of access point.
AP IP address, Ethernet MAC address, and Base Radio MAC address	IP address, Ethernet MAC address and Radio MAC address.
Country Code	The codes of the supported countries. Up to 20 countries can be supported per controller. **Note** Access points might not operate properly if they are not designed for use in your country of operation. For a complete list of country codes supported per product, see the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcscod.html.

Field	Description
Link Latency Settings	You can configure link latency on the controller to measure the link between an access point and the controller. See the Configuring Link Latency Settings for Access Points for more information. • Current Link Latency (in msec)—The current round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back. • Minimum Link Latency (in msec)—Because link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back. • Maximum Link Latency (in msec)—Because link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of heartbeat packets from the access point to the controller and back.
LWAPP/CAPWAP Uptime	Displays how long the LWAPP/CAPWAP connection has been active.
LWAPP?CAPWAP Join Taken Time	Displays how long the LWAPP/CAPWAP connection has been joined.
Admin Status	The administration state of the access point as either enabled or disabled.
AP Mode	
Local	Default mode. Data clients are serviced while configured channels are scanned for noise and rogues. The access point goes off-channel for 50 ms and listens for rogues. It cycles through each channel for the period specified under the Auto RF configuration. **Note** To configure Local or FlexConnect access points for the Cisco Adaptive wIPS feature, choose Local or FlexConnect and select the **Enhanced wIPS Engine Enabled** check box.

Field	Description
Monitor	Radio receive only mode. The access point scans all configured channels every 12 seconds. Only deauthenticated packets are sent in the air with an access point configured this way. A monitor mode access point can connect as a client to a rogue access point. **Note** To configure access points for Cisco Adaptive wIPS feature, select **Monitor**. Select the **Enhanced wIPS Engine Enabled** check box and choose **wIPS** from the Monitor Mode Optimization drop-down list. Before you can enable an access point to be in wIPS mode, you must disable the access point radios. If you do not disable the access point radio, an error message appears. **Note** Once you have enabled the access point for wIPS, reenable the radios.
Rogue Detector	The access point radio is turned off and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points heard over the network. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.
Sniffer	The access point captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. These packets contain information such as timestamp, signal strength, packet size, and so on. This feature can only be enabled if you run AiroPeek, which is a third-party network analyzer software that supports the decoding of data packets.
FlexConnect	Enables FlexConnect for up to six access points. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. **Note** FlexConnect must be selected to configure an OfficeExtend access point. When the AP mode is FlexConnect, FlexConnect configuration options display including the option to enable OfficeExtend AP and to enable Least Latency Controller Join.

Field	Description
Bridge	This is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The bridge and its wired clients are listed as client in the Prime Infrastructure if the AP mode is set to Bridge, and the access point is bridge capable.
Spectrum Expert	This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.
Enhanced wIPs Engine	Enabled or Disabled, to enable the monitoring of the security attacks using Cisco Adaptive wIPS feature.
Operational Status	Registered or Not Registered, as determined by the controller.
Registered Controller	The controller to which the access point is registered. Click to display the registered controller details. See the "Monitoring System Summary" section on page 5-4 for more information.
Primary Controller	The name of the primary controller for this access point.
Port Number	The SNMP name of the access point primary controller. The access point attempts to associate with this controller first for all network operations and in the event of a hardware reset.
AP Uptime	Displays how long the access point has been active to receive and transmit.
Map Location	Customer-definable location name for the access point. Click to look at the actual location on a map. Choose **Monitor** > **Access Points** > *name* > **Map Location** for more information.
Google Earth Location	Indicates whether a Google Earth location is assigned.
Location	The physical location where the access point is placed (or Unassigned).
Statistics Timer	This counter sets the time in seconds that the access point sends its DOT11 statistics to the controller.

Field	Description
PoE Status	The power over ethernet status of the access point. The possible values include the following: • Low—The access point draws low power from the Ethernet. • Lower than 15.4 volts—The access point draws lower than 15.4 volts from the Ethernet. • Lower than 16.8 volts—The access point draws lower than 16.8 volts from the Ethernet. • Normal—The power is high enough for the operation of the access point. • Not Applicable—The power source is not from the Ethernet.
Rogue Detection	Indicates whether or not Rogue Detection is enabled. **Note** Rogue detection is disabled automatically for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. For more information regarding OfficeExtend access points, see the *Cisco Wireless LAN Controller Configuration Guide*.
OfficeExtend AP	Indicates whether or not the access point is enabled as an OfficeExtend access point. The default is Enabled.
Encryption	Indicates whether or not encryption is enabled. **Note** Enabling or disabling encryption functionality causes the access point to reboot which then causes a loss of connectivity for clients. **Note** DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security. Encryption is only available if the access point is connected to a 5500 series controller with a Plus license.
Least Latency Join	The access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.
Telnet Access	Indicates whether or not Telnet Access is enabled.

Field	Description
SSH Access	Indicates whether or not SSH is enabled. **Note** An OfficeExtend access point might be connected directly to the WAN which could allow external access if the default password is used by the access point. Because of this, Telnet and SSH access are disabled automatically for OfficeExtend access points.
Versions	
Software Version	The operating system release.version.dot.maintenance number of the code currently running on the controller.
Boot Version	The operating system bootloader version number.
Inventory Information	
AP Type	Type of Access Point
AP Model	Access point model number.
Cisco IOS Version	The Cisco IOS Release details.
AP Certificate Type	Either Self Signed or Manufacture Installed.
FlexConnect Mode Supported	Indicates if FlexConnect mode is supported or not.
wIPS Profile (when applicable)	
Profile Name	Click the user-assigned profile name to view wIPS profile details.
Profile Version	
Unique Device Identifier (UDI)	
Name	Name of the Cisco AP for access points.
Description	Description of the access point.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial Number	Unique product serial number.

Field	Description
Run Ping Test Link— Click to ping the access point. The results are displayed in a pop-up dialog box. The below are the parameters associated: • Controller IP Address • Destination • Send Count • Received Count • Maximum Time Interval • Minimum Time Interval • Average Time Interval	
Alarms Link— Click to display alarms associated with this access point. • Severity • Message • Failure Source • Timestamp • Owner • Category • Condition	
Events Link— Click to display events associated with this access point. • Description • Failure Source • Timestamp • Severity • Category • Condition • Correlated	

General—Autonomous

Note   For autonomous clients, the Prime Infrastructure *only* collects client counts. The client counts in the Monitor page and reports have autonomous clients included. Client search, client traffic graphs, or other client reports (such as Unique Clients, Busiest Clients, Client Association) do *not* include clients from autonomous access points.

Table 5-48 lists the General (for Autonomous Access Points) tab fields.

Table 18: General (for Autonomous Access Points) Tab Fields

Field	Description
AP Name	Operator defined name of access point.
AP IP address and Ethernet MAC address	IP address, Ethernet MAC address of the access point.
AP UpTime	Indicates how long the access point has been up in number of days, hours, minutes, and seconds.
Map Location	Customer-definable location name for the access point. Click to look at the actual location on a map.
WGB Mode	Indicates whether or not the access point is in work group bridge mode.
SNMP Info	
SysObjectId SysDescription SysLocation SysContact	System Object ID. The system device type and current version of firmware. The physical location of the device, such as a building name or room in which it is installed. The name of the system administrator responsible for the device.
Versions	
Software Version	The operating system release.version.dot.maintenance number of the code currently running on the controller.
CPU Utilization	Displays the maximum, average, and minimum CPU utilization over the specified amount of time.
Memory Utilization	Displays the maximum, average, and minimum memory utilization over the specified amount of time.

Cisco Wireless Intrusion Prevention System Configuration Guide, Release 8.0

Field	Description
Inventory Information	
AP Type	Autonomous or lightweight.
AP Model	The Access Point model number.
AP Serial Number	Unique serial number for this access point.
FlexConnect Mode Supported	If FlexConnect mode is supported or not.
Unique Device Identifier (UDI)	
Name	Name of Cisco AP for access points.
Description	Description of access point.
Product ID	Orderable product identifier.
Version ID	Version of product identifier.
Serial Number	Unique product serial number.

Note Memory and CPU utilization charts are displayed.

Note Click **Alarms** to display the alarms associated with the access point. Click **Events** to display events associated with the access point.

Interfaces Tab

Table 5-49 lists the Interfaces tab fields.

Table 19: Interfaces Tab Fields

Field	Description
Interface	
Admin Status	Indicates whether the Ethernet interface is enabled.
Operational Status	Indicates whether the Ethernet interface is operational.
Rx Unicast Packets	Indicates the number of unicast packets received.

Field	Description
Tx Unicast Packets	Indicates the number of unicast packets sent.
Rx Non-Unicast Packets	Indicates the number of non-unicast packets received.
Tx Non-Unicast Packets	Indicates the number of non-unicast packets sent.
Radio Interface	
Protocol	802.11a/n or 802.11b/g/n.
Admin Status	Indicates whether the access point is enabled or disabled.
CleanAir Capable	Indicates whether the access point is able to use CleanAir.
CleanAir Status	Indicates the status of CleanAir.
Channel Number	Indicates the channel on which the Cisco Radio is broadcasting.
Extension Channel	Indicates the secondary channel on which Cisco radio is broadcasting.
Power Level	Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.
Channel Width	Indicates the channel bandwidth for this radio interface. See the Configuring 802.11a/n RRM Dynamic Channel Allocation for more information on configuring channel bandwidth. Minimum (default) setting is 20 MHz. Maximum setting is the maximum channel width supported by this radio.
Antenna Name	Identifies the type of antenna.

Click an interface name to view its properties (see Table 5-50).

Table 20: Interface Properties

Field	Description
AP Name	Name of the Access Point.
Link speed	Indicates the speed of the interface in Mbps.
RX Bytes	Indicates the total number of bytes in the error-free packets received on the interface.
RX Unicast Packets	Indicates the total number of unicast packets received on the interface.

Field	Description
RX Non-Unicast Packets	Indicates the total number of non-unicast or mulitcast packets received on the interface.
Input CRC	Indicates the total number of CRC error in packets received on the interface.
Input Errors	Indicates the sum of all errors in the packets while receiving on the interface.
Input Overrun	Indicates the number of times the receiver hardware was incapable of handing received data to a hardware buffer because the input rate exceeded the receiver capability to handle the data.
Input Resource	Indicates the total number of resource errors in packets received on the interface.
Runts	Indicates the number of packets that are discarded because they are smaller than the medium minimum packet size.
Throttle	Indicates the total number of times the interface advised a sending NIC that it was overwhelmed by packets being sent and to slow the pace of delivery.
Output Collision	Indicates the total number of packet retransmitted due to an Ethernet collision.
Output Resource	Indicates the total number of resource errors in packets transmitted on the interface.
Output Errors	Indicates the sum of all errors that prevented the final transmission of packets out of the interface.
Operational Status	Indicates the operational state of the physical Ethernet interface on the AP.
Duplex	Indicates the duplex mode of an interface.
TX Bytes	Indicates the total number of bytes in the error-free packets transmitted on the interface.
TX Unicast Packets	Indicates the total number of unicast packets transmitted on the interface.
TX Non-Unicast Packets	Indicates the total number of non-unicast or mulitcast packets transmitted on the interface.
Input Aborts	Indicates the total number of packet aborted while receiving on the interface.
Input Frames	Indicates the total number of packet received incorrectly having a CRC error and a non-integer number of octets on the interface.
Input Drops	Indicates the total number of packets dropped while receiving on the interface because the queue was full.

Field	Description
Unknown Protocol	Indicates the total number of packet discarded on the interface due to an unknown protocol.
Giants	Indicates the number of packets that are discarded because they exceed the maximum packet size of the medium.
Interface Resets	Indicates the number of times that an interface has been completely reset.
Output No Buffer	Indicates the total number of packets discarded because there was no buffer space.
Output Underrun	Indicates the number of times the transmitter has been running faster than the router can handle.
Output Total Drops	Indicates the total number of packets dropped while transmitting from the interface because the queue was full.

CDP Neighbors Tab

Table 5-51 lists the CDP Neighbors tab fields.

Note This tab is visible only when the CDP is enabled.

Table 21: CDP Neighbors Tab Fields

Field	Description
AP Name	The name assigned to the access point.
AP IP Address	IP address of the access point.
Port No	Port number connected or assigned to the access point.
Local Interface	Identifies the local interface.
Neighbor Name	Name of the neighboring Cisco device.
Neighbor Address	Network address of the neighboring Cisco device.
Neighbor Port	Port of the neighboring Cisco device.
Duplex	Indicates Full Duplex or Half Duplex.
Interface Speed	Speed at which the interface operates.

Current Associated Clients Tab

Table 5-52 lists the Current Associated Clients tab fields.

✎

Note   This tab is visible only when there are clients associated to the AP (CAPWAP or Autonomous AP).

Table 22: Current Associated Clients Tab Fields

Field	Description
Username	Click the username to view the Monitor Client Details page for this client. See the Monitoring Clients and Users for more information.
IP Address	IP address of the associated client.
Client MAC Address	Click the client MAC address to view the Monitor Client Details page for this client.
Association Time	Date and time of the association.
UpTime	Time duration of the association.
SSID	User-defined SSID name.
SNR (dB)	Signal to Noise Ratio in dB of the associated client.
RSSI	Received Signal Strength Indicator in dBm.
Bytes Tx	This indicates the total amount of data that has passed through the Ethernet interface either way.
Bytes Rx	This indicate the total amount of data that has been received through the Ethernet interface either way
When the access point is not associated with the controller, then the database is used to retrieve the data (rather than the controller itself). If the access point is not associated, the following fields appear.	
User Name	Username of the client.
IP Address	Local IP Address
Client MAC Address	Client MAC Address
Association Time	Timestamp of the client association.

Field	Description
Session Length	Time length of the session
SSID	User-defined SSID name.
Protocol	
Avg. Session Throughput	
Traffic (MB) as before	

> **Note** Click the **Edit View** link to add, remove or reorder columns in the Current Associated Clients table. See the "Configuring the List of Access Points Display" section on page 5-47 for adding a new field using the Edit View.

SSID Tab

Table 5-53 lists the SSID tab fields.

> **Note** This tab is visible only when the access point is Autonomous AP and there are SSIDs configured on the AP.

Table 23: SSID Tab

Field	Description
SSID	Service Set Identifier being broadcast by the access point radio.
SSID Vlan	SSID on an access point is configured to recognize a specific VLAN ID or name.
SSID Vlan Name	SSID on an access point is configured to recognize a specific VLAN ID or name.
MB SSID Broadcast	SSID broadcast disabled essentially makes your Access Point invisible unless a wireless client already knows the SSID, or is using tools that monitor or 'sniff' traffic from an AP's associated clients.
MB SSID Time Period	Within this specified time period, internal communication within the SSID continues to work.

Clients Over Time Tab

This tab displays the following charts:

- Client Count on AP—Displays the total number of clients currently associated with an access point over time.

- Client Traffic on AP—Displays the traffic generated by the client connected in the AP distribution over time.

Note The information that appears in the above charts is presented in a time-based graph. For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed. See the "Time-Based Graphs" section on page 6-71 for more information.

Generating Reports

In the Prime Infrastructure, you can generate various kinds of reports. This section explains how to generate Context Aware reports using the Prime Infrastructure Report Launch Pad. By default, reports are stored on the Prime Infrastructure server.

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

You can define the following criteria for the reports:

- 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 e-mailed or exported to a file

Report Launch Pad

The report launch pad provides access to all the Prime Infrastructure reports from a single page. In this page, you can view current reports, open specific types of reports, create and save new reports, and manage scheduled runs. You can access the ContextAware reports section in the Report Launch Pad to generate ContextAware reports.

Tip Hover your mouse cursor over the tool tip next to the report type to view more report details.

Creating and Running a New Report

To create and run a new report, follow these steps:

Step 1 Choose **Reports** > **Report Launch Pad**.
The reports are listed by category in the main section of the page and on the left sidebar menu.

Step 2 Find the appropriate report in the main section of the Report Launch Pad.
Note Click the report name from the Report Launch Pad or use the navigation on the left side of the Report Launch Pad page to view any currently saved reports for that report type.

Step 3 Click **New**. The Report Details page appears.

Step 4 In the Report Details page, enter the following Settings parameters:
Note Certain parameters may or may not appear depending on the report type.

- Report Title—If you plan to use this as a saved report, enter a report name.

- Report By—Choose the appropriate Report By category from the drop-down list.

- Report Criteria—Allows you to sort your results depending on the previous Report By selection made. Click Edit to open the Filter Criteria page.

  Note Click **Select to confirm your filter criteria** or Close to return to the previous page.

- Connection Protocol—All Clients, All Wired(802.3), All Wireless (802.11), All 11u Capable Clients, 802.11a/n, 802.11b/g/n, 802.11a, 802.11b, 802.11g, 802.11n (5 GHz), 802.11n (2.4 GHz).

- Reporting Period

  ◦ Select the reporting period from the Select a time period...drop-down list. The possible values are Today, Last 1 Hour, Last 6 Hours, Last 12 hours, Last 1 Day, Last 2 Days, Last 3 days, Last 4 Days, Last 5 Days, last 6 Days, Last 7 Days, Last 2 Weeks, Last 4 weeks, Previous Calendar Month, Last 8 Weeks, Last 12 Weeks, Last 6 Months, and Last 1 Year.

  ◦ From—Select the From radio button and enter the From and To dates and times. You can type a date in the text box, or click the Calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.

  ◦ Show—Enter the number of records that you want to be displayed on each page.

    Note Leave the text box blank to display all records.

Step 5 If you plan to run this report at a later time or as a recurring report, enter the Schedule parameters. The Schedule parameters allow you to control when and how often the report runs.

- Scheduling—Select the Enable check box to run the report on the set schedule.

- Export Format—Choose your format for exported files (CSV or PDF).

Cisco Wireless Intrusion Prevention System Configuration Guide, Release 8.0

• Destination—Select your destination type (File or E-mail). Enter the applicable file location or the e-mail address.

Note The default file locations for CSV and PDF files are as follows:

/localdisk/ftp/reports/Inventory/<ReportTitleName>_<yyyymmdd>_<HHMMSS>.csv

/localdisk/ftp/reports/Inventory/,ReportTitleName>_<yyyymmdd>_<HHMMSS>.pdf

Note To set the mail server setup for e-mails, choose Administration > Settings, then choose Mail Server from the left sidebar menu to view the Mail Server Configuration page. Enter the SMTP and other required information.

• Start Date/Time—Enter a date in the provided text box, or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists. The report begins to run on this data and at this time.

• Recurrence—Enter the frequency of this report.

  ◦ No Recurrence—The report runs only once (at the time indicated for the Start Date/Time).

  ◦ Hourly—The report runs on the interval indicated by the number of hours you enter in the Entry text box.

  ◦ Daily—The report runs on the interval indicated by the number of days you enter in the Every text box.

  ◦ Weekly—The report runs on the interval indicated by the number of weeks you enter in the Every text box and on the days specified by the selected check boxes.

  ◦ Monthly—The report runs on the interval indicated by the number of months you enter in the Every text box.

The Create Custom Report page allows you to customize the report results.

For the more information on the customizable reports, see *Cisco Prime Infrastructure User Guide*.

Step 6 Click **Customize** to open a separate Create Custom Report page.

a) From the Custom Report Name drop-down list, choose the report you intend to run. The Available and Selected column heading selections may change depending on the report selected.

b) From the Report View drop-down list, specify if the report should appear in tabular, graphical, or combined form (both). This option is not available on every report.

c) Use the Add > and < Remove buttons to move highlighted column headings between the two group boxes (Available data fields and Data fields to include).
   Note

   Column headings in blue are mandatory in the current sub report. They cannot be removed from the Selected Columns group box.

d) Use the Change Order buttons (Move Up or Move Down) to determine the order of the columns in the results table. The higher the column heading appears in the Selected Columns list, the farther left it appears in the results table.

e) In the Data field sorting group box, indicate your sorting preference (Ascending or Descending). Determine how the report data is sorted.

   • You can select four data fields for which you can specify sorting order. Use the Sort by and Then by drop-down lists to select each data field for sorting.

   • For each sorted data field, select whether you want it sorted in Ascending or Descending order.

   Note Only reports in table form (rather than graphs or combined) can be sorted. Only fields that can be sorted appear in the Data field sorting drop-down lists.

f) Click **Apply** to confirm the changes, **Reset** to return columns to the default, or **Cancel** to close this page with no changes made.

Note The changes made in the Create Custom Report page are not saved until you click Save in the Report Details page.

Step 7 When all report parameters have been set, choose one of the following:

- Save—Click **Save** to save this report setup without immediately running the report. The report automatically runs at the scheduled time.

- Save and Run—Click **Save and Run** to save this report setup and to immediately run the report.

- Run Now—Click **Run Now** to run the report without saving the report setup.

- Cancel—Click **Cancel** to return to the previous page without running nor saving this report.

Managing Current Reports

If a report has been saved for a specific report type, you can access the current reports from the Report Launch Pad.

When a new chokepoint is created, it is available in all the virtual domains. After placing it on a floor, it is updated so that it is available in the same virtual domain as that of a floor. When a chokepoint is removed from a floor, it will be available in all the virtual domains again.

To access current or saved reports from the Report Launch Pad, follow these steps:

Step 1 Choose **Reports** > **Report Launch Pad**

Step 2 Choose the specific report from the left sidebar menu or from the main section of the Report Launch Pad. The Report Launch Pad page displays a list of current reports for this report type.
To view a list of saved reports, choose **Reports** > **Saved Reports**.

Managing Scheduled Run Results

Note The list of scheduled runs can be sorted by report category, report type, and time frame.

Managing Saved Reports

In the Saved Reports page, you can create and manage saved reports. To open this page in the Prime Infrastructure, choose Reports > Saved Reports.

Note   The list of saved reports can be sorted by report category, report type, and scheduled status (enabled, disabled, or expired).

The Saved Reports page shows the following information:

- Report Title—Identifies the user-assigned report name. Click the report title to view the details for this report.

- Report Type—Identifies the specific report type.

- Scheduled—Indicates whether this report is enabled or disabled.

- Next Schedule On—Indicates the date and time of the next scheduled run for this report.

- Last Run—Indicates the date and time of the most recent scheduled run for this report.

- Download—Click the Download icon to open or save a .csv file of the report results.

- Run Now—Click the Run Now icon to immediately run the current report.

Creating a Device Utilization Report

To create a device utilization report for the Mobility Services Engine, follow these steps:

Step 1   Choose **Reports > Report Launch Pad**.

Step 2   Choose **Device > Utilization**.

Step 3   Click **New**. The Utilization Report Details page appears.

Step 4   In the Reports Details page, enter the following Settings parameters:
Note   Certain parameters may or may not work depending on the report type.

- Report Title—If you plan to save this report, enter a report name.

- Report Type—By default, the report type is selected as MSE.

- Report By—Choose the appropriate Report By category from the drop-down list. The categories differ for each report. See specific report sections for Report By categories for each report.

- Report Criteria—The parameter allows you to sort your results depending on the previous Report By selection made. Click **Edit** to open the Filter Criteria page.

- Connection Protocol—Choose from these protocols: **All Clients**, **All Wired (802.3)**, **All Wireless (802.11)**, **802.11a/n**, **802.11b/g/n**, **802.11a**, **802.11b**, **802.11g**, **802.11n (5-GHz)**, or **802.11n (2.4-GHz)**.

- SSID—All SSIDs is the default value.

- Reporting Period—You can define the report to collect data hourly, weekly, or at a specific date and time. The selected reporting period type is displayed on the x-axis.

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

Step 5   In the Schedule group box, select the **Enable Schedule** check box.

Step 6   Choose the report format (CSV or PDF) from the Export Report drop-down list.

Step 7   Select either **File** or **Email** as the destination of the report.

- If you select the File option, a destination path must first be defined in the **Administration > Settings** > **Report** page. Enter the destination path for the files in the Repository Path text box.

- If you select the Email option, an SMTP mail server must be defined prior to entry of target e-mail address. Choose **Administrator > Settings >** *Mail Server Configuration* to enter the appropriate information.

Step 8   Enter a start date (MM:DD:YYYY), or click the **Calendar** icon to select a date.

Step 9   Specify a start time using the hour and minute drop-down lists.

Step 10   Select the **Recurrence** radio button to determine how often you want to run the report. The possible values follow:

- No Recurrence

- Hourly

- Daily

- Weekly

- Monthly

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

Step 11   When finished with Step 1 to Creating a Device Utilization Report, do one of the following:

- Click **Save** to save edits. The report is run at the designated time and the results are either e-mailed or saved to a designated file as defined in the Schedule group box.

- 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 at the bottom of the page. The report also runs at the designated time and the results are either e-mailed or saved to a designated file as defined in the Schedule group box.

  ◦ In the results page, click **Cancel** to cancel the defined report.

- Click **Run Now** if you want to run the report immediately and review the results in the Prime Infrastructure page. The report runs regardless of any pending, scheduled run of that report. Results appear at the bottom of the page. Click **Save** if you want to save the report criteria that you entered.

Note You can also click **Run Now** to check the defined report criteria before saving it or to run reports as necessary. Only the CPU and memory utilization reports are shown in the following example.

Figure 25: Devise > MSE Utilization > Results
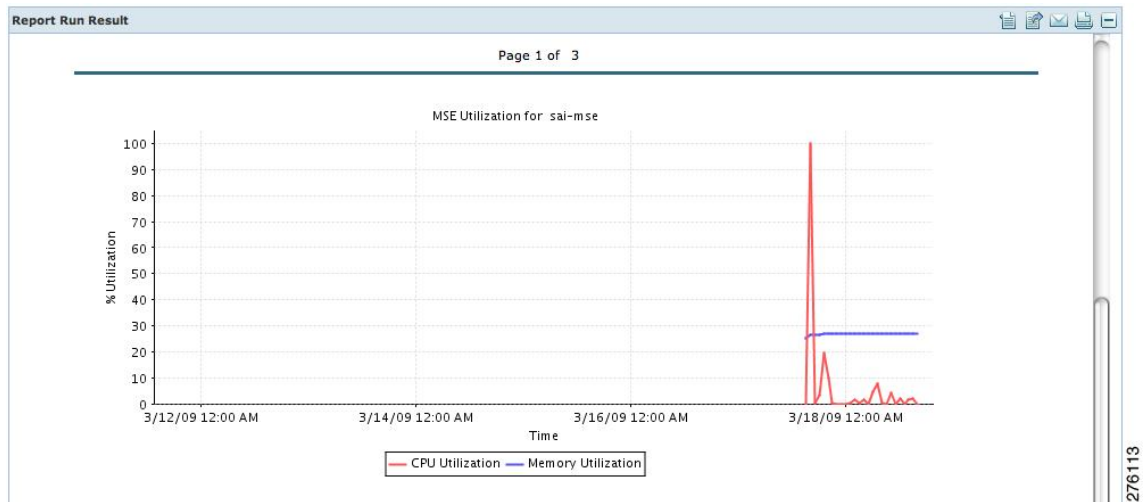
If the report is scheduled, it is shown as enabled and the next scheduled run date is noted.

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 12 To enable, disable, or delete a report, select the check box next to the report title, and click the appropriate option.

Viewing Saved Utilization Reports

To download a saved report, follow these steps:

Step 1 Choose **Reports > Saved Reports**.

Step 2 Click the **Download** icon for your report. It is downloaded and saved in the defined directory or e-mailed.

Viewing Scheduled Utilization Runs

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

Step 1   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, e-mailed.

Client Support on the MSE

You can use the Prime Infrastructure Advanced Search feature to narrow the client list based on specific categories and filters. You can also filter the current list using the Show drop-down list.

- Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address
- Viewing the Clients Detected by the MSE

Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address

To search for an MSE-located client using the Prime Infrastructure Advanced Search feature, follow these steps:

Step 1   Click **Advanced Search** located in the top right corner of the Prime Infrastructure UI.

Step 2   In the New Search dialog, choose **Clients** as the search category from the Search Category drop-down list.

Step 3   From the Media Type drop-down list, choose **Wireless Clients**.

           Note   The Wireless Type drop-down list appears only when you choose Wireless Clients as the media type.

Step 4   From the Wireless Type drop-down list, choose any of the following types: **All**, **Lightweight,** or **Autonomous Clients**.

Step 5   From the Search By drop-down list, choose **IP Address**.

           Note   Searching a client by IP address can contain either a full or partial IP address. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

Step 6   From the Clients Detected By drop-down list, choose **clients detected by MSE**.

This shows clients located by Context-Aware Service in the MSE by directly communicating with the Cisco WLCs.

Step 7   From the Last detected within drop-down list, choose the time within which the client was detected.

Step 8   Enter the client IP address in the Client IP Address text box. You can enter wither a partial or full IPv6 address.

           Note   If you are searching for the client from the Prime Infrastructure on the MSE by IPV4 address, enter the IPV4 address in the Client IP Address text box.

Step 9   From the Client States drop-down list, choose the client states. The possible values for wireless clients are **All States**, **Idle**, **Authenticated**, **Associated**, **Probing**, or **Excused**. The possible values for wired clients are **All States**, **Authenticated**, and **Associated**.

Step 10   From the Posture Status drop-down list, choose the posture status to know if the devices are clean or not. The possible values are **All**, **unknown**, **Passed**, and **Failed**.

Step 11   Select the **CCX Compatible** check box to search for clients that are compatible with Cisco Client Extensions. The possible values are **All Versions**, **V1**, **V2**, **V3**, **V4**, **V5**, and **V6**.

Step 12   Select the **E2E Compatible** check box to search for clients that are End to End compatible. The possible values are **All Versions**, **V1**, and **V2**.

Step 13   Select the **NAC State** check box to search for clients identified by a certain Network Admission Control (NAC) state. The possible values are **Quarantine**, **Access**, **Invalid**, and **Not Applicable**.

Step 14   Select the **Include Disassociated** check box to include clients that are no longer on the network but for which Prime Infrastructure has historical records.

Step 15   From the **Items per page** drop-down list, choose the number of records to be displayed in the search results page.

Step 16   Select the **Save Search** check box to save the selected search option.

Step 17   Click **Go**.
The Clients and Users page appears with all the clients detected by the MSE.

Viewing the Clients Detected by the MSE

To view all the clients detected by MSE, follow these steps:

Step 1   Choose **Monitor** > **Clients and Users** to view both wired and wireless clients information.
The Client and Users page appears.

The Clients and Users table shows a few column by default. If you want to display the additional columns that are available, click ⚙ ▾, and then click **Columns**. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.

Step 2   Filter the current list to choose all the clients that are detected by MSE by choosing **Clients detected by MSE** from the Show drop-down list.
All the clients detected by MSE including wired and wireless appear. All the clients detected by MSE including wired and wireless appear.

The following different parameters are available in the Clients Detected by MSE table:

  • MAC Address—Client MAC address.

    ◦ IP Address—Client IP address.

      The IP address that appears in the IP Address column is determined by a predefined priority order. The first IP address available in the following order appears in the IP address text box:

        ◦ IPv4 address

      Note   Only wireless clients have IPv6 addresses in this release. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

◦ IPv6 global unique address. If there are multiple addresses of this type, most recent IPv6 address that the client received is shown, because a user might have two Global IPv6 addresses but one might have been from an older Router Advertisement that is being aged out.

◦ IPv6 local unique address, if there are multiple then the most recent IPV6 local unique address is used by the client.

◦ IPv6 link local address. For an IPv6 address of the client which is self-assigned and used for communication before any other IPV6 address is assigned.

The following are the different IPv6 address types:

◦ Link-local Unicast—The link-local addresses are designed to be used for addressing on a single link for purposes such as auto-address configuration, neighbor discovery, or when no routers are present.

◦ Site-local Unicast—The site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix.

◦ Aggregatable Global Unicast—The aggregatable global unicast address uniquely identifies the client in global network and equivalent to public IPv4 address. A client can have multiple aggregatable global unicast addresses.

◦ IP Type—The IP address type of the client. The possible options are IPv4, IPv6, or Dual-stack that signifies a client with both a IPV4 and IPV6 addresses.

  ◦ Global Unique

  ◦ Unique Local

  ◦ Link Local

◦ User Name—Username based on 802.1x authentication. Unknown is displayed for client connected without a username.

◦ Type—Indicates the client type.

- Vendor—Device vendor derived from OUI.

- Device Name—Network authentication device name. For example, WLC and switch.

- Location—Map location of the connected device.

- VLAN—Indicates the access VLAN ID for this client.

- Status—Current client status.

  ◦ Idle—Normal operation; no rejection of client association requests.

  ◦ Auth Pending—Completing a AAA transaction.

  ◦ Authenticated—802.11 authenticated complete.

  ◦ Associated—802.11 association complete. This is also used by wired clients to represent that a client is currently connected to the network.

  ◦ Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.

- To Be Deleted—The client is deleted after disassociation.

- Excluded—Automatically disabled by the system due to perceived security threat.

- Interface—Cisco WLC interface (wireless) or switch interface (wired) that the client is connected to.

- Protocol

  - 802.11—Wireless

  - 802.3—Wired

- Association Time—Last association start time (for wireless client). For a wired client, this is the time when a client is connected to a switch port. This is blank for a client which is associated but has problems being on the network.

- CCX—Lightweight wireless only.

  - Select the radio button next to MAC Address in the Client and User page to view the associated client information. The following client parameters appear:

- Client attributes

- Client IPV6 Addresses

- Client Statistics

  Note   Client Statistics shows the statistics information after the client details are shown.

- Client Association History

- Client Event Information

- Client Location Information

- Wired Location History

- Client CCX Information

- Client Attributes

When you choose a client from the Clients and Users list, the following client details are displayed. Clients are identified using the MAC address.

- General—Lists the following information:

  - User Name

  - IP Address

  - MAC address

  - Vendor

  - Endpoint Type

  - Client Type

  - Media Type

◦ Mobility Role

◦ Hostname

◦ E2E

◦ Foundation Service

◦ Management Service

◦ Voice Service

◦ Location Service

- Session—Lists the following information:

   ◦ Controller Name

   ◦ AP Name

   ◦ AP IP Address

   ◦ AP Type

   ◦ AP Base Radio MAC

   ◦ Anchor Address

   ◦ 802.11 State

   ◦ Association ID

   ◦ Port

   ◦ Interface

   ◦ SSID

   ◦ Profile Name

   ◦ Protocol

   ◦ VLAN ID

   ◦ AP Mode

- Security (wireless and Identity wired clients only)—Lists the following security information:

   ◦ Security Policy Type

   ◦ EAP Type

   ◦ On Network

   ◦ 802.11 Authentication

   ◦ Encryption Cipher

   ◦ SNMP NAC State

   ◦ RADIUS NAC State

◦ AAA Override ACL Name

◦ AAA Override ACL Applied Status

◦ Redirect URL

◦ ACL Name

◦ ACL Applied Status

◦ FlexConnect Local Authentication

◦ Policy Manager State

◦ Authentication ISE

◦ Authorization Profile Name

◦ Posture Status

◦ TrustSec Security Group

◦ Windows AD Domain

Note   The identity clients are clients whose authentication type is 802.1x, MAC Auth Bypass, or Web Auth. For non-identity clients, the authentication type is N/A.

Note   The data that appears under the client attributes differs based on identity and non-identity clients. For identity clients, you can see the security information such as Authentication status, Audit Session ID, and so on.

• Statistics (wireless only)

• Traffic—Shows the client traffic information.

• For wireless clients, client traffic information comes from the Cisco WLC. For wired clients, the client traffic information comes from the ISE, and you must enable accounting information and other necessary functions on the switches.

Statistics

The **Statistics** group box contains the following information for the selected client:

• Client AP Association History.

• Client RSSI History (dBm)—History of RSSI (Received Signal Strength Indicator) as detected by the access point with which the client is associated.

• Client SNR History—History of SNR (signal-to-noise ratio of the client RF session) as detected by the access point with which the client is associated.

• Bytes Sent and Received (Kbps)—Bytes sent and received with the associated access point.

• Packets Sent and Received (per sec)—Packets sent and received with the associated access point.

• Client Data rate

This information is presented in interactive graphs.

Client IPV6 Addresses

The Client IPv6 Address group box contains the following information for the selected client:

- IP Address—Shows the client IPv6 address.
- Scope—Contains 3 scope types: Global Unique, Local Unique, and Link Local.
- Address Type—Shows the address type.
- Discovery Time—Time when the IP was discovered.

    Association History

    The association history group box shows information regarding the last ten association times for the selected client. This information helps in troubleshooting the client.

    ◦ Association Time
    ◦ Duration
    ◦ User Name
    ◦ IP Address
    ◦ IP Address Type
    ◦ AP Name
    ◦ Controller Name
    ◦ SSID

      Events

The Events group box in the Client Details page displays all events for this client including the event type as well as the date and time of the event:

- Event Type
- Event Time
- Description

  Map

Click **View Location History** to view the location history details of wired and wireless clients.

The following location history information is displayed for a wired or wireless client:

- Timestamp
- State
- Port Type
- Slot
- Module
- Port
- User Name
- IP Address

• Switch IP

• Server Name

• Map Location Civic Location

Monitoring Geo-Location

The MSE provides physical location of wired clients, wired endpoints, switches, Cisco WLCs, and access points present in a wireless network deployment. Currently, MSE provides location information in geo-location format to the external entities through northbound and southbound entities.

To improve the accuracy of the geo-location information provided by MSE, this feature aims to transform the geometric location co-ordinates of a device to geo-location coordinates (latitude and longitude) and provides it to the external entities through northbound and southbound interfaces.

Note   At least three GPS markers are required for geo-location calculation. The maximum number of GPS markers that you can add is 20.

Adding a GPS Marker to a Floor Map

To add a GPS marker to a floor map, follow these steps:

Step 1   Choose **Monitor** > **Site Maps** to display the Maps page.

Step 2   Choose **Campus Name** > **Building Name** > **Floor Name**.

Step 3   Choose the **Add/Edit GPS Markers** Information menu option on the top left menu to open the Add/Edit GPS page. A GPS Marker icon appears on the top left corner of the map (X=0 Y=0).

Step 4   You can drag the GPS Marker icon and place it in the desired location on the map or enter the X and Y position values in the GPS Marker Details table on the left sidebar menu to move the marker to the desired position.

Note   If the markers added are too close, then the accuracy of geo-location information is less.

Step 5   Enter the Latitude and Longitude degrees for the selected GPS Marker icon in the left sidebar menu.

Step 6   Click **Save**.
The GPS Marker information is saved to the database.

Step 7   Click **Apply to other Floors of Building** to copy GPS markers on one floor of a building to all the remaining floors of that building.

Editing a GPS Marker

To edit a GPS marker present on the floor, follow these steps:

Step 1   Choose **Monitor** > **Site Maps** to display the Maps page.

Step 2   Choose **Campus Name** > **Building Name** > **Floor Name**.

Step 3   Choose the **Add/Edit GPS Markers Information** menu option to open the Add/Edit GPS page.

Step 4   Select an existing GPS Marker which is present on the floor from the left sidebar menu.

Step 5   From the left sidebar menu, you can change the Latitude, Longitude, X Position, and Y Position which is associated with the GPS marker.

Step 6   Click **Save**.
The modified GPS marker information is now saved to the database.

Deleting a GPS Marker From the Floor

To delete a GPS marker from the floor, follow these steps:

Step 1   Choose **Monitor** > **Site Maps** to display the Maps page.

Step 2   Choose **Campus Name** > **Building Name** > **Floor Name**.

Step 3   Choose the **Add/Edit GPS Markers Information** menu option to open the Add/Edit GPS page.

Step 4   Select an existing GPS marker that is present on the floor from the left sidebar menu.
Note   You can delete multiple GPS markers present on a floor by selecting the **Multiple GPS Markers** check box.

Step 5   Click **Delete GPS Marker**.
The selected GPS marker is deleted from the database.

Ekahau Site Survey Integration

Ekahau Site Survey (ESS) tool is used for designing, deploying, maintaining, and troubleshooting high performance Wi-Fi networks. ESS works over any 802.11 network and is optimized for centrally managed 802.11n Wi-Fi networks.

You can use the ESS tool to import the existing floor maps from the Prime Infrastructure and export the project to the Prime Infrastructure. For more information, see the Cisco Prime Infrastructure Integration section in the ESS online help.

Note The Prime Infrastructure site survey calibration requires that you have collected at least 150 survey data points at 50 distinct locations. If you do not have enough survey data points, a warning is given when trying to export the survey data.

Note If there are no access points in the Prime Infrastructure during the site survey, the site survey will not happen.

Note If the floor map scales are incorrect in the Prime Infrastructure, the visualizations in the ESS will be distorted.

AirMagnet Survey and Planner Integration

AirMagnet survey and AirMagnet planner is integrated with the Cisco Prime Infrastructure. This integration increases the operational efficiencies by eliminating the need to repeat the wireless planning and site survey tasks commonly associated with deployment and management of wireless LAN networks.

The AirMagnet survey tool allows you to export real world survey data to the Prime Infrastructure for calibrating planner modeling. With the AirMagnet planner, you can create and export planner projects directly to the Prime Infrastructure. This enables the Prime Infrastructure to create its own project directly from the imported AirMagnet Planner tool. For more information, see the AirMagnet Survey and Planning documentation which is available at Fluke Networks website.

Interpreting Security Dashboard

The Prime Infrastructure Security Dashboard have the following features added to it:

- Valid Client on Rogue AP

- Soft AP

- Good Guy Gone Bad (GGGB)

All the above features falls under the Client Classification table on the security dashboard. Hyperlinks are provided for the counts of Rogue APs. By clicking on the hyperlinks provided in the table, you will be able to view the details of Soft AP, GGGB and Valid Client on Rogue.

Viewing the Rogue APs

To view the Rogue Access Points (APs), perform the following steps:

SUMMARY STEPS

1. Click the **Valid Client connected to Rogue AP** number to view the clients who were previously associated with the enterprise network but are now associated with Rogue APs.
2. This page displays the following items:
3. Click the **Soft AP** number to view the clients who were previously probing but are now rogue APs.
4. This page displays the following items:
5. Click the **Good Guy Gone Bad** number to view the clients who were previously associated but are now Rogue APs.
6. This page displays the following items:

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	Click the **Valid Client connected to Rogue AP** number to view the clients who were previously associated with the enterprise network but are now associated with Rogue APs.	
Step 2	This page displays the following items:	• Client Mac Address- Mac address of the client • Rogue AP Mac Address- Mac address of the rogue APs. • First Detected- Displays the date and time when a rogue AP was first detected • Last Detected- Displays the date and time when a rogue AP was last detected • Containment Start Time • Containment Stop Time • State- The state of the rogue AP when a Valid client is connected to rogue. The two states are, Alert and Threat
Step 3	Click the **Soft AP** number to view the clients who were previously probing but are now rogue APs.	
Step 4	This page displays the following items:	• Type- Displays the type of the client • Soft AP MAC Address- Mac address of the Soft AP • TimeStamp- Displays the exact date and time when a soft AP was detected
Step 5	Click the **Good Guy Gone Bad** number to view the clients who were previously associated but are now Rogue APs.	
Step 6	This page displays the following items:	• Type- Displays the type of the client

Command or Action	Purpose
	• Good Guy Gone Bad Mac Address- Mac address of the Good Guy Gone Bad client
	• TimeStamp- Displays the exact date and time when a soft AP was detected

Client Classification

There are three clients:

Valid Client Connected to Rogue AP: When a client associates with rogue AP, MSE will check whether the client is a valid client. For valid clients, an entry is added to the Rogue AP table with the MAC addresses of both the devices. Depending on the containment action taken, containment fields are updated. The following scenarios needs to be considered:

- Client associates and then disappears
- Client dissociation information is available
- Incomplete Containment

Soft AP: A Soft Access Point (Soft AP) is set-up on a Wi-Fi adapter without the need of a physical Wi-Fi router. It is easy to set-up a Soft AP on the Windows 7 or Windows Vista Machine with Windows 7 virtual Wi-Fi capabilities. Once up and running, it is easy to share the network access available on a machine to other Wi-Fi users that will connect to the Soft AP. If an employee sets up a soft Access Point on his machine inside the corporate premises, and share the corporate network through it, then this soft AP behaves as Rogue AP. You can also turn on Wi-Fi tethering on your smartphone and act as a rogue AP. MSE detects this scenario of soft rogue AP and sends response to Controller for auto containment.

Good Guy Gone Bad: When a valid client turns into a Soft AP, it is a greater threat which need s immediate action. MSE detect s these scenarios and report s a good guy gone bad.

PART II

Cisco MSE Admin User Interface

CHAPTER **8**

Cisco MSE Admin User Interface

- MSE Admin UI Home Page, page 157

- Using Data Accuracy Tool, page 160

- Monitoring System and Network Health, page 162

MSE Admin UI Home Page

The MSE admin UI home page displays at-a-glance views of the most important data in your network, status of various services, and allows you to configure MSE system settings. You can also view the Beta version of various applications such as the Health and Data Accuracy Tool by choosing **admin > enable beta features** in the top right side of the page.

Launching the MSE Admin User Interface

To launch the MSE admin user interface, follow these steps:

SUMMARY STEPS

1. Launch the MSE admin user interface (UI). To launch it, type https://*mseip*/*mseui* in the Web Browser or you can launch it from the Cisco Prime Infrastructure (PI) by clicking the MSE name link from **Services > Mobility Services Engines** page.

2. Enter the username and password.

3. Click **Sign In**.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Launch the MSE admin user interface (UI). To launch it, type https://*mseip*/*mseui* in the Web Browser or you can launch it from the Cisco Prime Infrastructure (PI) by clicking the MSE name link from **Services** > **Mobility Services Engines** page.	**Note** The MSE admin UI is displayed only if you have selected the MSE Admin View check box in the Administration > User Preference Page from the Prime Infrastructure user interface.
Step 2	Enter the username and password.	
Step 3	Click **Sign In**.	The MSE admin UI home page appears.

MSE Services

This section briefly describes the different services that the Cisco MSE supports within the overall Cisco Unified Wireless Network (CUWN):

All the available services are listed in the MSE admin UI home page under the Services group box.

- **CMX Analytics** —The CMX Analytics service analyzes wireless device location information in a particular network. The CMX Analytics service uses the data provided by the Cisco Mobility Services Engine (MSE) to calculate the location of Wi-Fi devices in the Wireless Local Area Network (WLAN). When a wireless device is enabled in a network, it transmits probe request packets to identify the wireless network in its neighborhood. Even after connecting to the access point in the WLAN, the client devices continue to transmit probe request packets to identify other access points for better quality of service. The access points gather these request and the associated RSSI from the various wireless devices and forwards them to the Wireless LAN Controller (WLC). The controller then forwards this information to the MSE.

  The basic data that is collected from various APs, when analyzed, produces information and knowledge about the movement and behavior patterns of people who are using Wi-Fi devices in the building. For example, the building can be an airport, shopping mall, city center, and so on. The CMX Analytics service helps the airport authorities or the building owners to understand the movement of passengers or customer within their building. This helps them improve the signage, make changes to the under utilized areas, and so on.

- **Context Aware Service**—Also known as Location service. This is the core service of the Mobility Services Engine (MSE) that turns on Wi-Fi client tracking and location API functionality. Allows MSE to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as presence, location, telemetry data, and historical information.

- **CMX Connect & Engage**—Connect and Engage Service—Formerly known as Browser Engage Service. The CMX Connect and Engage service provides connect, a guest Wi-Fi on-boarding solution, zone, and message configuration for the CMX Software Development Kit (SDK).

- **Mobile Concierge**—Mobile Concierge enables the Cisco Mobility Services Advertisement Protocol (MSAP). This protocol enables direct communication between the MSE and mobile devices, allowing content to be pushed directly to the mobile device pre-association. This functionality is dependent on the mobile device supporting 802.11u and MSAP.

• **Wireless Intrusion Prevention**—Provides wireless-specific network threat detection and mitigation against malicious attacks, security vulnerabilities, and sources of performance disruption within the CUWN infrastructure. wIPS visualizes, analyzes, and identifies wireless threats, and centrally manages mitigation and resolution of security and performance issues using Cisco monitor mode and Enhanced Local Mode (ELM) Access Points. Proactive threat prevention is also supported to create a hardened wireless network core that is impenetrable by most wireless attacks.

Enabling or Disabling the MSE Services

To enable or disable the MSE services, follow these steps:

SUMMARY STEPS

1. Launch the MSE Admin UI.
2. To enable any of the services, follow these steps:
3. To disable any of the services, follow these steps:

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	Launch the MSE Admin UI.	The MSE Admin UI home page appears. The following are the various services displayed in the Services group box: • CMX Analytics • Context Aware Service • CMX Connect & Engage • Mobile concierge • Wireless Intrusion Prevention
Step 2	To enable any of the services, follow these steps:	**Note** Services that are enabled will be in green color and the disabled services will in red color. • Click the desired services tab that you wish to enable in the Services group box. • Click the **Up/Down** button. Do you really want to change the service status dialog box appears. • Click **Ok**. The color of the **Up** button changes to green once the service is enabled. Also the corresponding service name in the Services group box changes to green.
Step 3	To disable any of the services, follow these steps:	• Click the desired services tab that you wish to disable in the Services group box. • Click the **Up/Down** button. Do you really want to change the service status dialog box appears. • Click **Ok**.

Command or Action	Purpose
	The color of the **Down** button changes to red once the service is disabled. Also the corresponding services name in the Services group box changes to red.

MSE Applications

The admin UI is composed of the following web applications which serve as the front end for the services:

- What's New
- CMX Connect and Engage
- Maps
- Data Accuracy Tool
- Health

Using Data Accuracy Tool

Prerequisites

Before you filter the devices using location tuning or device filters, you should do the following using Cisco Prime Infrastructure user interface:

- Synchronize the floor area of a building with the MSE.
- Draw Perimeter on the floor.

For more information on synchronization and map editors, see chapter Monitoring Maps in *Cisco Prime Infrastructure Classic View Configuration Guide*.

Working with Location Tuning

To filter the devices outside the venue, follow these steps:

Step 1   Launch the MSE admin UI.

Step 2   Choose **admin > Enable Beta Features** to view the beta features.

Step 3   Click the **Data Accuracy Tool** tile.
The location tuning page appears.

Step 4   Choose a campus name from the drop-down list.

Step 5   Choose a building name from the drop-down list.

Step 6   Choose a building floor from the drop-down list.

Step 7   Click **Show Map**.
The floor map appears.

Step 8   Click **Inside Training**.

Step 9   Enter the comma separated MAC addresses of the devices roaming inside the perimeter area drawn on the floor.

Step 10   Click **Start Data Collection** to start collecting data for the devices within the perimeter area.
Minimum 100% data collection is required to create a model. 100 % represents at least 20 RSSI reading per operational AP present on the floor.

Step 11   Click **Outside Training**.

Step 12   Enter the comma separated MAC addresses of the devices roaming outside the area drawn on the floor.

Step 13   Click **Start Data Collection** to start collecting data for the devices outside the perimeter area.
Minimum 100% data collection is required to create a model. This 100% is considering the inside training data also.

Step 14   Click **Create Model** to create a model based on the collected data.
To enable **Create Model** button, you should stop the data collection when 100% data collection is complete. To delete all the collected data, click **Delete Data**.

Filtering Devices Based on Maximum RSSI Threshold

To filter the devices, follow these steps:

Step 1   Launch the MSE admin UI.

Step 2   Choose **admin > Enable Beta Features** to view the beta features.

Step 3   Click the **Data Accuracy Tool** tile.

Step 4   Click the **Device Filters** tab.

Step 5   Choose a building name from the drop-down list.

Step 6   Choose a building floor from the drop-down list.

Step 7   Choose a zone in the floor.

Step 8   Select Max RSSI Threshold from the report drop-down list.

Step 9   Enter the comma separated MAC addresses of the devices available in the selected zone.

Step 10   Select a RSSI threshold value.

Step 11   Click **View**.
It takes up to 10 minutes to show the data.

You will be able to view the RSSI report for the devices.

Filtering Devices Based on Stationary Devices and MAC Addresses

To filter the devices, follow these steps:

Step 1   Launch the MSE admin UI.

Step 2   Choose **admin > Enable Beta Features**.

Step 3   Click the **Data Accuracy Tool** tile.

Step 4   Click the **Device Filters** tab.

Step 5   Choose a building name from the drop-down list.

Step 6   Choose a floor of the building.

Step 7   Choose a zone in the floor.

Step 8   Choose Stationary Devices and MAC Addresses from the report drop-down list.

Step 9   Enter the comma separated MAC addresses of the devices available in the selected zone.

Step 10   Select the duration.

Step 11   Click **View**.
You will be able to view the MAC addresses of the located devices.

This allows you to download the report of stationary devices.

Monitoring System and Network Health

Viewing Health Dashboard

To view health dashboard for a specific mobility services engine, follow these steps:

Step 1   Choose **Services > Mobility Services**.

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

Step 3   Click **Health** tile from the MSE admin UI home page.

Step 4   Choose **Application Statistics > Health Dashboard**.
You can view the utilization percentage of CPU, system memory, disk space, analytics CPU, analytics memory, CAS CPU and CAS memory.

Viewing CAS Latency Statistics

To view CAS latency statistics information for a specific mobility services engine, follow these steps:

Step 1   Choose **Services > Mobility Services**.

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

Step 3   Click **Health** tile from the MSE admin UI home page.

Step 4   Choose **Application Statistics > CAS Latency Statistics**.
You will be able to view the CAS latency statistics, CAS queue delay and CAS calculation time.

Viewing Notification Statistics

To view notification statistics information for a specific mobility services engine, follow these steps:

Step 1   Choose **Services > Mobility Services**.

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

Step 3   Click **Health** tile from the MSE admin UI home page.

Step 4   Choose **Application Statistics > Notification Statistics**.
The following table lists fields in the Notification Statistics page.

Field	Description
Destination Summary	
Total Destinations	Destinations total count.
Unreachable Destinations	Unreachable destinations count.
Statistics Summary	
Host Address	The destination IP address to which the notifications are sent.
Port	The destination port to which the notifications are sent.
Destination Type	The type of the destination. Example: SOAP_XML.
Status	Status of the destination device. The status is either Up or Down.
Last Sent	The date and time at which the last notification was sent to the destination device.

Field	Description
Last Failed	The date and time at which the notification had failed.
Track Definition (Status)	Track definition can be either Nothbound or CAS event notification.
Total Count	The total count of notifications sent to the destination. Click the count link to view the notification statistics details of the destination device.

Viewing Vital Statistics

To view vital statistics information for a specific mobility services engine, follow these steps:

Step 1   Choose **Services > Mobility Services**.

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

Step 3   Click **Health** tile from the MSE admin UI home page.

Step 4   Choose **Application Statistics > Vital Statistics**.
You can view the graphical representation of vital statistics over a period of time.

Configuring MSE System Settings and Services

Viewing General Properties and Enabling Services

To view the general properties and enable the MSE services, follow these steps:

Step 1   Launch the MSE admin UI.

Step 2   Click the Configuration icon on the top right of the home page.

Step 3   Choose **System** > **General Properties** from the left sidebar menu.
The General Properties page appears. This table lists the General Properties page fields.

Table 24: General Tab

Field	Configuration Options
Model	Model details for the MSE.
Build	The software version running on the MSE.
UDI	The Device UDI (Unique Device Identifier) is the string between double quote characters (including spaces in the end if any).
IP Address	Indicates the IP address for the Mobility Services Engine.
Hostname	Hostname.
Mobility Services	To enable a service on the Mobility Services Engine, select the check box next to the service. The services include Context Aware, wIPS, Mobile Concierge, CMX Analytics, CMX Browser Engage, and Proxy service. You can choose CAS to track clients, rogues, interferers, wired clients, and tags. Choose either of the following engines to track tags: • Cisco Tag Engine or • Partner Tag Engine **Note** The Partner Tag Engine is used only to track the tags. The clients are still tracked by Cisco Context-Aware Engine. **Note** Once selected, the service is displayed as Up (active). All inactive services are noted as Down (inactive) on the selected (current) system and on the network. **Note** From release 7.5 onward, wIPS service requires a dedicated MSE because it does not support CAS and wIPS on the same MSE. Click the **here** link to see the number of devices that can be assigned for the current system. In the License Center page, choose **MSE** from the left sidebar menu option to see the license details for all Mobility Services Engines on the network. **Note** For more information on purchasing and installing licenses, see the following URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html
Current Server Time	Current time on the server.
Server Time Zone	Current time zone the server is located in.
Server Start Time	Indicates the start time when the server was started.

Field	Configuration Options
Server Restarts	Number of times the server has restarted.
Maximum Memory (MB)	Maximum memory installed on the MSE.
Allocated Memory (MB)	Maximum memory available to the MSE.
Used Memory (MB)	Maximum memory being used by the MSE.
DB Disk Usage (GB)	Amount of data in the MSE database disk.
CAS Element Limit (licensed)	Number of elements (Clients, tags, interferes, etc) that the MSE is licensed to track.
Current Active Element Count	Number of elements (clients, tags, interferers, etc) that the MSE is currently tracking.
Elements not tracked due to limiting	Number of elements above the licensed limit on the MSE.

Step 4   Click **Save** to update the Prime Infrastructure and Mobility Services Engine databases.

Viewing Dashboard

To view the dashboard, follow these steps:

Step 1   Launch the MSE admin UI.

Step 2   Click the Configuration icon on the top right of the home page.

Step 3   Choose **System > Dashboard**.
You will be able to view the following details in the dashboard:

- No of active clients
- Percentage of memory utilization
- Percentage of CPU utilization
- Notification Destinations
- MAC Filtering Status - Enabled or Disabled
- Client Location History - Enabled or Disabled
- Location calculation latency
- Type of license used
- Number of controllers synched

Viewing and Adding License

To view and add license to the MSE, follow these steps:

Step 1   Launch the MSE admin UI.

Step 2   Click the Configuration icon on the top right of the home page.

Step 3   From the left sidebar menu, choose **System > Licensing**.

Step 4   The License page displays the following information.

Field	Description
Type	Type of service.
Platform Limit	Platform Limit
Installed Limit	Displays the total number of client elements licensed across MSEs.
License Type	The three different types of licenses. They are permanent, evaluation, and extension.

Step 5   Click **Select File** to browse for the license file.

Step 6   Click **Add** to add the license to the MSE.

Viewing Active Sessions on a System

You can view active user sessions on the Mobility Services Engine.

To view active user sessions, follow these steps:

Step 1   Launch the MSE admin UI.

Step 2   Click the Configuration icon on the top right of the home page.

Step 3   Choose **System > Active Sessions**.
For every session, the Prime Infrastructure shows the following information:

- Session identifier

- IP address from which the MSE is accessed

- Username of the connected user

• Date and time when the session started

• Date and time when the MSE was last accessed

• How long the session was idle since it was last accessed

Adding Trap Destinations

To add a trap destination, follow these steps:

Step 1   Launch the MSE admin UI.

Step 2   Click the Configuration icon on the top right of the home page.

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

Step 4   Click **Add Trap Destination**.
The following table lists the Add Trap Destination page fields.

Table 25: Add Trap Destination Page Fields

Field	Description
IP Address	IP address for the trap destination.
Port	The port number for the trap destination. The default port number is 162.
Community	SNMP community string for the trap destination.
Destination Type	This field is not editable and has a value of **Other**.
SNMP Version	Choose either **v2c** or **v3** from the SNMP Version drop-down list.
The following set of fields appear only if you select v3 as the SNMP version.	
User Name	The username for the SNMP Version 3.
Security Name	The security name for the SNMP Version 3.
Authentication Type	Choose one of the following from the drop-down list: **HMAC-MD5** **HMAC-SHA**
Authentication Password	The authentication password for the SNMP Version 3.

Field	Description
Privacy Type	Choose one of the following from the drop-down list: **CBC-DES** **CFB-AES-128** **CFB-AES-192** **CFB-AES-256**
Privacy Password	The privacy password for the SNMP Version 3.

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

Step 5   Click **Save**.
You are returned to the Trap Destination Summary page and the newly defined trap is listed.

Deleting Trap Destinations

To delete a trap destination, follow these steps:

Step 1   Launch the MSE admin UI.
Step 2   Click the Configuration icon on the top right of the home page.
Step 3   Choose **System > Trap Destinations**.
Step 4   Click the Delete icon corresponding to the trap destination entry that you want to delete.
Step 5   In the dialog box that appears, click **OK** to confirm deletion.

Viewing Advanced Parameter Settings

To view the advanced parameter settings of the Mobility Services Engine, follow these steps:

Step 1   Launch the MSE admin UI.
Step 2   Click the Configuration icon on the top right of the home page.
Step 3   Choose **System** > **Advanced Parameters**. The Advanced Parameters page appears.

Configuring Advanced Parameters

To configure advanced parameters, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 From the left sidebar menu, choose **System > Advanced Parameters**.

Step 4 View or modify the advanced parameters as necessary.

- ◦ Number of Days to keep Events—Enter the number of days to keep logs. Change this value as required for monitoring and troubleshooting.

  ◦ Session Timeout—Enter the number of minutes before a session times out. Change this value as required for monitoring and troubleshooting. Currently this option appears dimmed.

- Advanced Commands

  ◦ Reboot Hardware—Click to reboot the mobility services hardware. See the Rebooting or Shutting Down a System, on page 46 for more information.

  ◦ Shutdown Hardware—Click to turn off the mobility services hardware. See the Rebooting or Shutting Down a System, on page 46 for more information.

  ◦ Clear Database—Click to clear the mobility services database. See the Clearing the System Database, on page 46 for more information. Unselect the **Retain current service assignments in Prime Infrastructure** check box to remove all existing service assignments from the Prime Infrastructure and MSE. The resources must be reassigned in the **Services** > **Synchronize Services** page. By default, this option is selected.

Step 5 Click **Save** to update the Prime Infrastructure and Mobility Services Engine databases.

Rebooting or Shutting Down a System

To reboot or shut down a Mobility Services Engine, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **System > Advanced Parameters**.

Step 4 In the Advanced Commands group box, click the appropriate button (**Reboot Hardware** or **Shutdown Hardware**). Click **OK** in the confirmation dialog box to initiate either the reboot or shutdown process. Click **Cancel** to stop the process.

Clearing the System Database

To clear a Mobility Services Engine configuration and restore its factory defaults, follow these steps:

Step 1   Launch the MSE admin UI.

Step 2   Click the Configuration icon on the top right of the home page.

Step 3   Choose **System > Advanced Parameters**.

Step 4   In the Advanced Commands group box, click **Clear Database**.

Step 5   Click **OK** to clear the Mobility Services Engine database.

Configuring Logging Options

You can use Prime Infrastructure to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

Step 1   Launch the MSE admin UI.

Step 2   Click the Configuration icon on the top right of the home page.

Step 3   Choose **System > Logging**. The logging options for the selected Mobility Services Engine appear.

Step 4   Choose the appropriate options from the Logging Level drop-down list.
There are four logging options: **Off**, **Error**, **Information**, and **Trace**.

All log records with a log level of **Error** or above are logged to a new error log file locserver-error-%u-%g.log. This is an additional log file maintained along with the location server locserver-%u-%g.log log file. The error log file consists of logs of **Error** level along with their context information. The contextual information consists of 25 log records prior to the error. You can maintain up to 10 error log files. The maximum size allowed for each log file is 10 MB.

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

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

Step 6   Select the **Enable** check box under Advanced Parameters to enable advanced debugging. By default, this option is disabled.
Caution   Enable advanced debugging only under the guidance of Cisco TAC personnel because advanced debugging slows the mobility service down.

Step 7   To download log files from the server, click **Download Logs**. For more information, see the Downloading Log Files.

Step 8   In the Log File group box, enter the following:

- The number of log files to be maintained in the Mobility Services Engine. You can maintain a minimum of 5 log files and a maximum of 20 log files in the Mobility Services Engine.

- The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.

Step 9   In the MAC Address Based Logging page, do the following:

- Select the **Enable** check box to enable MAC address logging. By default, this option is disabled.

- Add one or more MAC addresses for which you want to enable logging. You can also remove MAC addresses that you have already added by selecting the MAC address from the list and clicking **Remove**.

  For more information on MAC-address-based logging, see the MAC address-based Logging.

Step 10   Click **Save** to apply your changes.

Downloading Log Files

If you need to analyze Mobility Services Engine log files, you can use Prime Infrastructure to download them to your system. The Prime Infrastructure downloads a .zip file containing the log files.

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

Step 1   Launch the MSE admin UI.

Step 2   Click the Configuration icon on the top right of the home page.

Step 3   Choose **System > Logging**.

Step 4   Click **Download Logs**.

Step 5   Follow the instructions in the File Download dialog box to view the file or save the .zip file to your system.

wIPS Policy Alarm Encyclopedia

Security IDS/IPS Overview

The addition of WLANs to the corporate environment introduces a new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured and unconfigured access points and DoS (Denial of Service) attacks.

The Cisco Wireless IPS (wIPS) is designed to help manage against security threats by validating proper security configurations and detecting possible intrusions. With the comprehensive suite of security monitoring technologies, the wIPS alerts the user on more than 100 different threat conditions in the following categories:

- User authentication and traffic encryption
- Rogue and ad-hoc mode devices
- Configuration vulnerabilities
- Intrusion detection on security penetration
- Intrusion detection on DoS attacks
- Performance Violation

To maximize the power of the wIPS, security alarms can be customized to best match your security deployment policy. For example, if your WLAN deployment includes access points made by a specific vendor, the product can be customized to generate the rogue access point alarm when an access point made by another vendor is detected by the access point or sensor.

User Authentication and Encryption

The first line of defense for WLAN security is user authentication and wireless traffic encryption. Centralized WLAN user authentication based on the IEEE 802.1x standard with a RADIUS server at the back-end is a flexible and strong mechanism. Other authentication methods such as VPN may also be used to achieve the same goals.

User authentication blocks out unauthorized access to the wired and wireless resources. Traffic encryption goes hand-in-hand with user authentication during which the encryption secrets are exchanged between AP and authorized users. Traffic encryption prevents intruders from eavesdropping into the wireless traffic. Cisco wIPS validates your WLAN security deployment by monitoring on the authentication transactions and traffic encryption methods against the specified security deployment policy, which Cisco wIPS learns from the policy configuration. For example, the Cisco wIPS generates the **Device unprotected by PEAP** alarm if the **802.1x EAP** type-**PEAP** is the enterprise standardized authentication protocol. Common security violations in this category (authentication and encryption) include mis-configurations, out-of-date software/firmware, and suboptimal choice of corporate security policy. Cisco wIPS alerts the administrator on these issues and provides counter measures.

User Authentication and Encryption includes the following two subcategories:

Static WEP Encryption

Static WEP encryption was specified in the IEEE 802.11 standard in 1999. For security sensitive WLAN deployments, other alternatives such as WPA (Wireless Protected Access - TKIP and 802.1x) and 802.11i exist to address the encryption tasks.

Statistics show that more than 50 percent of WLANs do not implement any encryption method. Even with the potential vulnerability of static WEP, it is still safer than no encryption at all. If you decide to use static WEP, there are ways to keep it as secure as WEP can provide. Cisco wIPS assists you in accomplishing this goal by monitoring on static WEP usage and identifying security holes such as crackable WEP key usage, shared-key authentication, and detecting devices that do not use WEP.

Static WEP Encryption include the following types:

AP with Encryption Disabled

Alarm Description and Possible Causes

Cisco wIPS alerts the administrator on any AP operating without any WLAN layer 2 data encryption mechanisms such as **WEP, TKIP,** or **AES**. **VPN** technologies at layer three and above are the most commonly used alternative to the WLAN layer 2 data encryption mechanisms . If neither of the encryption mechanisms are used, data exchanged between an AP and its client stations is subject to eavesdropping by intruders. For an AP that is operating without any sort of encryption mechanism, there can be unauthorized clients without encryption keys that can associate with the AP and obtain access to the enterprise wired network. This puts at risk not only the user data privacy but also exposes the corporate wired network access. This alarm may be turned off for the enterprise guest WLAN network or for hot spot deployments where encryption is not required. You can turn on the Publicly Secure Packet Forwarding (**PSPF**-term generally used by Cisco Aironet access points. Other vendors may call this differently) alarm to protect your wireless network operating without any encryption. **PSPF** is a feature implemented on the WLAN Access Points to block wireless clients from communicating with other wireless clients. PSPF protects public networks by prohibiting wireless traffic between wireless clients.

wIPS Solution

Cisco wIPS detects wireless clients communicating with other wireless clients and alerts the administrator on a possible Publicly Secure Packet Forwarding (PSPF) violation. For most WLAN environments, the wireless clients mostly communicate only with devices such as web servers on the wired network. Enabling the PSPF feature on an Access Point, the administrator can protect wireless clients from being hacked by another wireless intruder. PSPF is very effective when implemented at wireless public networks (hotspots) such as airports, hotels, coffee shops, college campuses, etc. where there is no authentication and any one can associate with the APs. PSPF prevents client devices from inadvertently sharing files with other client devices on the wireless network.

Client with Encryption Disabled

Alarm Description and Possible Causes

Cisco wIPS alerts the administrator on any client station operating without any WLAN layer 2 data encryption mechanisms such as WEP, TKIP, or AES. VPN technologies at layer three and above are the most commonly used alternative to the WLAN layer 2 data encryption mechanisms . If neither of the encryption mechanism is used, data exchanged between an AP and its client stations is subject to eavesdropping by intruders. Clients with WEP disabled put at risk their file system that may contain confidential corporate information from wireless intruders. These clients can then act as an entry point for the intruders into the corporate network. This alarm may be turned off for the enterprise guest WLAN network or for hot spot deployments where encryption is generally not required. It is advisable to turn on the PSPF (Publicly Secure Packet Forwarding-term generally used by Cisco Aironet access points. Other vendors may call this differently) alarm to protect your wireless network operating without any encryption. PSPF is a feature implemented on the WLAN Access Points to block wireless clients from communicating with other wireless clients.

wIPS Solution

Cisco wIPS detects wireless clients communicating with other wireless clients and alerts the administrator on a possible PSPF violation. For most WLAN environments, the wireless clients mostly communicate only with devices such as web servers on the wired network. Enabling the PSPF feature on an Access Point, the administrator can protect wireless clients from being hacked by another wireless intruder. PSPF is very effective when implemented at wireless public networks (hotspots) such as airports, hotels, coffee shops, college campuses, etc. where there is no authentication and any one can associate with the APs. PSPF prevents client devices from inadvertently sharing files with other client devices on the wireless network.

Crackable WEP IV key used

Alarm Description and Possible Causes

WLAN devices using static WEP key for encryption are vulnerable to WEP key cracking attack. The WEP secret key that has been cracked by any intruder results in no encryption protection, thus leading to compromised data privacy. The WEP key which is in 64-bit or 128-bit (few vendors also offer 152-bit encryption) consists of the secret key specified by the user concatenated with the 24-bit IV (Initialization Vector). The IV that is determined by the transmitting station can be reused frequently or in consecutive frames, thus increasing the possibility of the secret key to be recovered by wireless intruders. By excluding certain IV values that would create "weak keys," the weakness of WEP is avoided.

wIPS Solution

Cisco wIPS alerts on weak WEP implementations and recommends a device firmware upgrade if available from the device vendor to correct the IV usage problem. Ideally, enterprise WLAN networks can protect against WEP vulnerability by using the Temporal Key Integrity Protocol (TKIP) encryption mechanism,

which is supported by most enterprise level wireless equipment. TKIP enabled devices are not subject to any WEP key attacks.

Device Using Open Authentication

Alarm Description and Possible Causes

802.11 Open Authentication (as opposed to Shared-key authentication) is widely used today in conjunction with a higher level authentication protocol such as 802.1x to secure a WLAN. In some deployments, Shared-key Authentication is used instead of Open Authentication where a static WEP key is used to challenge client stations attempting to associate with the AP. Open Authentication on the other hand accepts associations from any client and there is no verification of the identity of the client. Shared-key authentication appears to be more secure but has been proven to be vulnerable to WEP key cracking by wireless intruders because the challenge text and response are both clear and unencrypted.

wIPS Solution

It is always recommended to use 802.11 Open Authentication with some higher level authentication mechanisms such as the 802.1x/EAP framework or VPN. In case your deployment chooses to use Shared-key Authentication or something other than Open Authentication, you can enable this alarm . Cisco wIPS alerts you on any device that violates the deployment policy of not using Open Authentication.

Device Using Shared Key Authentication

Alarm Description and Possible Causes

The IEEE 802.11 standard designed the Shared-key Authentication protocol to work with static WEP key encryption to lock out unauthorized WLAN devices from associating with an AP or ad-hoc station. The Shared key authentication uses a standard challenge and response approach for authentication between the 802.11 client and the access point. The challenge text is unencrypted and in clear text. The algorithm (not the shared secret key) for the challenge response is standard and public knowledge. It has been proven that shared key authentication can be easily exploited through a passive attack by eavesdropping. An attacker can use brute force to compute the challenge response off-line after capturing challenge text, which is in clear text. Once the match is found, the attacker has acquired the shared secret key.

wIPS Solution

Cisco wIPS detects the use of Shared Key Authentication and advises alternatives. Many enterprises today deploy 802.11 WLANs using Open Authentication instead of Shared Key Authentication with a higher level authentication mechanism provided by 802.1x and EAP methods such as LEAP, PEAP and TLS .

WEP IV Key Reused

Alarm Description and Possible Causes

The WEP secret key that has been cracked by any intruder results in no encryption protection, thus leading to compromised data privacy. The WEP key which in most cases is 64-bit or 128-bit (few vendors also offer 152-bit encryption) consists of the secret key specified by the user concatenated with the 24-bit IV (Initialization Vector). The IV that is determined by the transmitting station can be reused frequently in consecutive frames, thus increasing the possibility of the secret key to be recovered by wireless intruders.

wIPS Solution

Cisco wIPS alerts on weak WEP implementations and recommends a device firmware upgrade if available from the device vendor to correct the IV usage problem. Ideally, enterprise WLAN networks can protect against WEP vulnerability by using the Temporal Key Integrity Protocol (TKIP) encryption mechanism,

which is now supported by most enterprise level wireless equipment. TKIP enabled devices are not subject to any such WEP key attacks.

WPA and 802.11i

The Wi-Fi published Wireless Protected Access (**WPA**) specification identifies a feature subset of the IEEE **802.11i** standard. WPA is one of the answers to the well publicized vulnerability of static WEP as specified by the original IEEE 802.11 specification. Most wireless vendors supports **WPA** and consider it to be a more secure alternative to static **WEP**.

There are three major end user benefits provided by the **WPA** products:

- **802.1x** allows user based authentication instead of the vulnerable global encryption key method.

- Temporal Key Integrity Protocol (**TKIP**) enhances industrial strength encryption with dynamic keying.

- Pre-shared Master Key (**PMK**) offers small and medium size deployment to use **802.1x** and **TKIP** without complex infrastructure back-end servers such as **RADIUS**

The wIPS server monitors **WPA** transactions and alerts the administrator when it detects non-compliant devices and weak configurations.

WPA and 802.11i include the following types:

Device Unprotected by EAP-TTLS

Alarm Description and Possible Causes

The Extensible Authentication Protocol (EAP) is a basic security framework which provides a means for improving the encryption of 802.11 transactions. This framework can be paired with a wide variety of different types of authentication mechanisms, including a version known as Tunneled Transport Layer Security (TTLS). EAP-Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends Transport Layer Security (TLS). EAP-TTLS provides security that is as strong as EAP-TLS but doesn't require the clients to be issued certificates. User authentication is still performed via passwords, but the credentials are tunneled. Devices configured to use the EAP protocol but not the TTLS authentication mechanism can represent potential insecure connections to the wireless network. Although such mechanisms make it easier for end-users to get connected quickly, wireless attackers may also be able to gain access to critical corporate data . EAP exchanges that are not secured by TTLS authentication can be easier for attackers to intercept and decode, potentially resulting in sensitive leakage of data sent from a valid user.

wIPS Solution

Cisco wIPS monitors EAP transactions to detect any devices that are not implementing the EAP-TTLS mechanism and triggers an alarm to notify administrators of the vulnerability. The alarm text provided on the AirWISE screen will identify the problematic device as well as the alternative authentication mechanism in use. It is recommended that IT personnel locate the device triggering the alarm and configure it to use the EAP-TTLS mechanism.

Device Unprotected by 802.1X

Alarm Description and Possible Causes

If your WLAN security deployment requires the use of 802.1x for authentication and encryption, Cisco wIPS alerts you on devices that are not configured to use 802.1x protection. Wireless Protected Access (**WPA**) specified 802.1x as one of the requirements. The 802.1x framework provides centralized user authentication

and encryption key management. The 802.1x is used with a variety of Extensible Authentication Protocol (**EAP**) types such as Lightweight Extensible Authentication Protocol(**LEAP**),Transport Layer Security(**TLS**),Tunneled Transport Layer Security(**TTLS**), Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (**EAP-FAST**) and Protected Extensible Authentication Protocol (**PEAP**) to implement an authentication and encryption mechanism. If your WLAN security relies on WPA or 802.1x, APs not configured for 802.1x weaken your WLAN security by allowing non-compliant users to falsely authenticate and enter your wired network. Mis-configured client stations without 802.1x protection also introduce security risks. For example, it would not have the mutual authentication mechanism provided by 802.1x framework and therefore be vulnerable to accidentally associate with an intruder's fake AP.

wIPS Solution

Cisco wIPS recognizes all 802.1x **EAP** types including **PEAP, TLS, TTLS, LEAP, EAP-FAST**, Cisco wIPS detects APs and client stations unprotected by 802.1x by observing rejected 802.1x authentication challenges.

Device Unprotected by any Selected Authentication Methods

Alarm Description and Possible Causes

Cisco wIPS monitors on 802.1x transactions and their specific Extensible Authentication Protocol (EAP) methods. When a specific EAP method is not used, Cisco wIPS will trigger an alarm. Cisco wIPS supports the following EAP methods for this alarm:

- Leap - This is a proprietary EAP method developed by Cisco. The Cisco LEAP solution provides mutual authentication, dynamic per session and per user keys and configurable WEP session key time out.

- PEAP - The Protected Extensible Authentication Protocol, is also known as Protected EAP. It is a protocol that encapsulates EAP within a potentially encrypted and authenticated Transport Layer Security (TLS) tunnel.

- EAP-TLS - EAP-Transport Layer Security (EAP-TLS). The EAP-TLS mechanism provides additional security over standard shared-key password authentication sessions by creating a new key on a per-session basis.

- EAP-TTLS - EAP-Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends TLS. EAP-TTLS provides security that is as strong as EAP-TLS but doesn't require the clients to be issued certificates. User authentication is still performed via passwords, but the credentials are tunneled.

- EAP-FAST - Cisco Systems has developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol. In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is then authenticated using the user-name and password credentials.

- EAP-MD5 - This is a password based authentication method that offers minimal security. EAP-MD5 differs from other EAP methods by providing authentication of the EAP peer to the EAP server but not the mutual authentication.

wIPS Solution

Cisco wIPS monitors EAP transactions to detect any devices that are not implementing the enabled authentication methods and triggers an alarm to notify administrators of the vulnerability. The alarm text provided on the AirWISE screen will identify the problematic device. It is recommended that IT personnel locate the device triggering the alarm and configure it to use the correct authentication method.

802.1 X Unencrypted Broadcast or Multicast

Alarm Description and Possible Causes

802.1x has a framework allowing a system to use per-session encryption keys to defend against the weakness inherited from the global static WEP key mechanism. 802.1x provide per-session encryption keys and also facilitates the session key rotation mechanism there by ensuring that the encryption keys are updated periodically. This enhances security by eliminating the use of static encryption keys and preventing attacks that require the collection of large amounts of data encrypted with a single static key. For multicast and broadcast packets, where there are multiple recipients, per-session encryption key cannot be applied. In order to secure multicast and broadcast communication, a shared encryption key and re-key mechanism has to be implemented. It has been found that very few wireless devices implement the multicast and broadcast encryption key mechanism correctly. In reality, multicast and broadcast packets are not encrypted. To make matters more complicated, enterprise grade APs with multiple SSIDs are frequently deployed with 802.1x security for one SSID (corporate WLAN) and no encryption for another SSID (guest WLAN). This deployment scenario is usually coupled with the VLAN configuration so that client devices using the guest SSID can only access the Internet but not the corporate wired network. An AP supporting multiple SSIDs transmits broadcast and multicast frames thus making the encryption option selection (802.1x or no encryption) , an implementation challenge.

wIPS Solution

Cisco wIPS detects unencrypted multicast and broadcast frames caused by mis-configuration or vendor implementation errors. Cisco recommends that the user should use APs that implement the encryption of multicast and broadcast frames in a proper manner.

802.1 X Rekey Timeout Too Long

Alarm Description and Possible Causes

A cracked WEP secret key results in no encryption protection so, data privacy will have to be compromised. Dynamic encryption key or key rotation mechanisms such as Temporal Key Integrity Protocol (TKIP) resolves such vulnerabilities by periodically changing the encryption key even within a single session. Managing key rotation for multicast and broadcast traffic is challenging technically because multiple devices have to update to the new key synchronously. Vendors' implementations of multicast or broadcast key rotation varies from null to complete. When the multicast and broadcast key is not rotated or rotated infrequently, it is as weak as static WEP, which is subject to key recovery attacks. By continuously monitoring on the WLAN 802.1x authentication and encryption transactions, Cisco wIPS can detect an AP configured without encryption key rotation or configured with a long key rotation timeout. It is important for WLAN 802.1x configurations to include a reasonable encryption rekey timeout . A staled encryption key makes your encryption static and as vulnerable as static WEP key encryption. A rekey mechanism should be applied to unicast, multicast, and broadcast data streams. TKIP enabled devices implement a WEP key hashing algorithm and typically rotate keys on their unicast data streams but not always on the multicast or broadcast data streams.

wIPS Solution

This Cisco wIPS alarm assists you in enforcing rekey mechanism for all data streams. Take appropriate steps including the checking of the AP configuration for this setting to tackle the issue.

Device Not Protected by EAP-TLS

Alarm Description and Possible Causes

The Extensible Authentication Protocol (EAP) is a basic security framework which provides a means for improving the encryption of 802.11 transactions. This framework can be paired with a wide variety of different types of authentication mechanisms, including a version known as Transport Layer Security (TLS), a certificate-based protocol. The EAP-TLS mechanism provides additional security over standard shared-key password authentication sessions by creating a new key on a per-session basis. This means that every active connection to an AP utilizing EAP-TLS authentication creates a new shared key specific to that connection. This makes the protocol significantly stronger than the standard shared-key mechanisms against wireless attackers. Devices configured to use the EAP protocol and not the TLS authentication mechanism, can represent potential insecure connections to the wireless network. There are a number of alternative mechanisms that may be used (such as EAP-TTLS or EAP-FAST) which generally provide greater convenience than EAP-TLS at the cost of reduced security for the network. Although such mechanisms make it easier for end-users to get connected quickly, wireless attackers may also be able to gain access to critical corporate data. EAP exchanges that are not secured by TLS authentication can be easier for attackers to intercept and decode, resulting in sensitive data leakage sent from a valid user.

wIPS Solution

Cisco wIPS monitors EAP transactions to detect devices that are not implementing the TLS mechanism and triggers an alarm to notify administrators of the vulnerability. The alarm text provided on the AirWISE screen will identify the problematic device as well as the alternative authentication mechanism in use. It is recommended that IT personnel locate the device triggering the alarm and configure it to use the EAP-TLS mechanism.

Device Unprotected by IEEE 802.11i/AES

Alarm Description and Possible Causes

The new 802.11i standard provides three critical network security capabilities:- authentication and privacy. Cisco wIPS alerts on detecting devices that are not using the IEEE 802.11i standard. Devices that are not using this security standard could be vulnerable to various attacks, compromising the enterprise network's security. When the IEEE 802.11 standard was ratified it suggested the implementation of the 64-bit WEP key as a security standard. Later it was increased to 128 bit keys. Some implementations were using upto 256 bit WEP keys. Since then, Static WEP has been proved to be flawed with respect to authentication, encryption and integrity checks. Soon the Wi-Fi alliance realized the importance of having an alternative to the WEP standard. The IEEE 802.11i standard was introduced to mitigate all the security issues that have been plaguing the wireless networks in the enterprise environment. This standard creates Robust Secure Networks (RSN). As the 802.11i standard would not be ratified in time, the Wi-FI Alliance created a subset of the IEEE 802.11i standard called Wi-Fi Protected Access (WPA).WPA/802.11i implements 802.1x for user authentication and key distribution. 802.1x is used with a variety of**EAP** (Extensible Authentication Protocol) types such as **LEAP, TLS, TTLS, EAP-FAST** and **PEAP** to implement an authentication and encryption mechanism. The IEEE 802.11i standard leaves it upto the user to select the authentication scheme.

The IEEE 802.11i standard provides a pre-shared key (PSK) mechanism and the 802.1x-server based key management schemes. The server based mechanism requires an authentication server such as a RADIUS server to securely and dynamically distribute session keys (Pairwise Master Key or PMK). When PSK is used instead of 802.1x, the passphrase PSK is converted via a formula into a 256-bit value needed for the PMK. In the PSK mode, the 802.11i defined 4-way handshake is used for encryption key management, with no EAP exchange. As there is no RADIUS server and no EAP methods (EAP-TLS, LEAP) involved, the PSK mode is less secure. There are two encryption standards defined in the IEEE 802.11i standard- Temporal Key

Integrity Protocol (TKIP) and Advanced Encryption Standard-Counter Mode-CBC MAC Protocol. WLAN traffic encrypted with TKIP and MIC defeats packet forgery, and replay attack. TKIP is most importantly immune to the weakness introduced by a static WEP key and attacks stemming from key reuses. Along with MIC, TKIP also provides per packet key mixing which helps prevent many keystream attacks.

The implementation of AES-CCMP is mandatory for the IEEE 802.11i standard. The IEEE standard supports only the 128-bit AES. As AES is supposed to work on 128-bit blocks, CCMP provides the padding necessary to increase the bit size for the data block. This padding is added before encryption and is discarded after the decryption. AES-CCMP mode provides authentication and encryption using the AES block cipher. CCMP is a combination of the Counter (CTR) mode encryption for data privacy, and Cipher Block Chaining Message Authentication Code (CBC-MAC) authentication, for an authenticate-and-encrypt security process for each data block processed. CCMP computes the CBC-MAC over the IEEE 802.11 header length, selected parts of the IEEE 802.11 MAC Payload Data Unit (MPDU) header, and the plaintext MPDU data, whereas the old IEEE 802.11 WEP mechanism provided no protection to the MPDU header. Second, both CCMP encryption and decryption use only the forward AES block cipher function leading to significant savings in code and hardware size.

wIPS Solution

Cisco wIPS detects devices that are not using the IEEE 802.11i standard and compromising the security of the wireless network. Cisco wIPS recommends the user to take the appropriate steps to avoid any security holes in the network and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard. Once such device is identified and reported by Cisco wIPS, the WLAN administrator may use the device locator feature provided on the Cisco wIPS Console to locate the device if it is a rogue device. Known devices can be marked as Monitored node and then located using the Triangulation feature.

Device Unprotected By EAP-FAST

Alarm Description and Possible Causes

Cisco Systems has developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol which will stop these dictionary attacks. EAP-FAST helps prevent Man-in-the-middle attacks, dictionary attacks, packet and authentication forgery attacks. In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is then authenticated using the user-name and password credentials. Some of the major advantages of EAP-FAST are that it is not proprietary, is compliant with the IEEE 802.11i standard, supports TKIP and WPA, does not use certificates thus avoiding complex PKI infrastructures and supports multiple Operating Systems on the PCs and the Pocket PCs.

wIPS Solution

Cisco wIPS alerts the wireless administrator on devices that are using the 802.1x authentication mechanism but are not using the EAP-FAST protocol. It is recommended that EAP-FAST be implemented in the wireless environment.

Device Unprotected by PEAP

Alarm Description and Possible Causes

Cisco wIPS monitors on **802.1x** transactions and their specific Extensible Authentication Protocol (**EAP**) types. By adopting Protected EAP (**PEAP**) as your authentication method, your 802.1x security authentication protocol will be further wrapped and protected by TLS (Transport Layer Security). EAP methods running within PEAP are provided with built-in advantages on the following:

- Identity protection

- Dictionary attack resistance

- Protected negotiation from replay attack

- Header protection

- Protected termination from packet spoofing, flooding, and denial-of-service attack

- Fragmentation and re-assembly

- Fast reconnect

- Proven and method independent key management

Many WLAN equipment vendors including Cisco have recently added support for PEAP with a firmware upgrade.

wIPS Solution

This Cisco wIPS alarm alerts you on devices that are not using Protected Extensible Authentication Protocol (**PEAP**). Ensure that the PEAP authentication method is implemented on various devices in the wireless environment.

Device Unprotected by TKIP

Alarm Description and Possible Causes

The latest **IEEE 802.11i** standard includes Temporal Key Integrity Protocol (**TKIP**) and Message Integrity Checksum(**MIC**) as one of the recommended data privacy protocols. WiFi Alliance also recommends **TKIP** and **MIC** in its (Wireless Protected Access (**WPA**) specification. WLAN traffic encrypted with **TKIP** and **MIC** defeats packet forgery, and replay attack. **TKIP** is immune to the weakness introduced by a static WEP key and attacks stemming from key reuses. Along with **MIC, TKIP** also provides per packet key mixing which helps prevent many keystream attacks. Unlike **AES** based **CCMP** encryption, TKIP typically does not require a hardware upgrade. Many WLAN equipment vendors including Cisco have added TKIP and MIC support in their latest firmware and driver.

wIPS Solution

Cisco wIPS detects WLAN traffic that is not protected by TKIP encryption and raises an alarm for attention. Cisco wIPS advises updating these devices to the latest firmware and re-configuring them to include TKIP encryption.

WPA or 802.11i Pre-Shared Key Used

Alarm Description and Possible Causes

WPA and the **802.11i** standard provide a pre-shared key (**PSK**) mechanism as an alternative to using the IEEE 802.1x-based key establishment. 802.1x-based key management requires an authentication server such as a **RADIUS** server to securely and dynamically distribute session keys (Pairwise Master Key or **PMK**). When **PSK** is used instead of 802.1x, the passphrase **PSK** is converted via a formula into a 256-bit value needed for the Pairwise Master Key. In the **PSK** mode, the 802.11i defined 4-way handshake is used for encryption key management, with no **EAP** exchange. As there is no **RADIUS** server and no **EAP** methods (EAP-TLS, LEAP) involved, the PSK mode is less secure. **PSK** is used to eliminate the need to set up an authentication server (RADIUS) but at the cost of reduced security. The 802.11i specification specifies that security can be considered weak if the pass phrase is less than 20 characters as it can be easily broken via an off-line dictionary attack once the 4-way handshake is captured. The problem is that vendors do not provide any easy-to-use tool that can generate and manage 20 character passphrases.

wIPS Solution

Cisco wIPS detects the use of the pre-shared key (**PSK**) mode and recommends switching to the more secure 802.1x EAP based key management and authentication system. If you decide to stay with **PSK** mode key management, please make sure your choice of the pass phrase is longer than 20 characters and does not comprise of words from a dictionary, thus preventing possible attacks.

Intrusion Detection—Denial of Service Attack

Wireless DoS (denial of service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLAN at Layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example, an RF jamming attack with a high power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

The nature and protocol standards for wireless are subject to some of these attacks. Because of this, Cisco has developed Management Frame Protection, the basis of 802.11i, to proactively prevent many of these attacks. (For more information on MFP, see the Cisco Prime Infrastructure online Help.) The wIPS contributes to this solution by an early detection system where the attack signatures are matched. The DoS of the wIPS detection focuses on WLAN layer one (physical layer) and two (data link layer, 802.11, 802.1x). When strong WLAN authentication and encryption mechanisms are used, higher layer (IP layer and above) DoS attacks are difficult to execute. The wIPS server tightens your WLAN defense by validating strong authentication and encryption policies. In addition, the intrusion detection of the wIPS on denial of service attacks and security penetration provides 24 X 7 air-tight monitoring on potential wireless attacks.

Denial of service attacks include the following three subcategories:

Denial of Service Attack Against Access Points

DoS attacks against access points are typically carried out on the basis of the following assumptions:

- Access points have limited resources. For example, the per-client association state table.

- WLAN management frames and authentication protocols 802.11 and 802.1x have no encryption mechanisms.

Wireless intruders can exhaust access point resources, most importantly the client association table, by emulating large number of wireless clients with spoofed MAC addresses. Each one of these emulated clients attempts association and authentication with the target access point but leaves the protocol transaction mid-way. When the access points resources and the client association table is filled up with these emulated clients and their incomplete authentication states, legitimate clients can no longer be serviced by the attacked access point. This creates a denial of service attack.

The wIPS tracks the client authentication process and identifies DoS attack signatures against the access point. Incomplete authentication and association transactions trigger the attack detection and statistical signature

matching process. Detected DoS attack results in setting off wIPS alarms, which includes the usual alarm detail description and target device information.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing. For more information on MFP, see the Prime Infrastructure online Help.

DoS attacks against access points include the following types:

Alarm Description and 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.

wIPS Solution

The Cisco Adaptive Wireless IPS detects spoofed MAC addresses and tracks the follow-up 802.1x actions and data communication after a successful client association to detect this form of DoS attack. After this attack is reported by the Cisco Adaptive Wireless IPS, you may log on to this access point to inspect its association table for the number of client associations.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing. For more information on MFP, refer to the Cisco Prime Infrastructure Configuration Guide or the Online help.

 •

Denial of Service Attack: Association Table Overflow

Alarm Description and Possible Causes

Wireless intruders can exhaust access point resources, most importantly the client association table, by imitating a large number of wireless clients with spoofed MAC addresses. Each one of these imitated clients attempts association and authentication with the target access point. The 802.11 authentication typically completes because most deployments use 802.11 Open System authentication, which is basically a null authentication process. Association with these imitated clients follows the authentication process. These imitated clients do not, however, follow up with higher level authentication such as 802.1x or VPN, which would leave the protocol transaction half-finished. At this point, the attacked access point maintains a state in the client association table for each imitated client. Once the access point's resources and client association table is filled with these imitated clients and their state information, legitimate clients can no longer be serviced by the attacked access point. This creates a DoS (denial of service) attack.

wIPS Solution

The Cisco Adaptive Wireless IPS tracks the client authentication process and identifies a DoS attack signature against an access point. Incomplete authentication and association transaction trigger the Cisco Adaptive Wireless IPS's attack detection and statistical signature matching process.

Denial of Service Attack: Authentication Flood

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement such a state machine according to the IEEE standard (see illustration below). On the access point, each client station has a state recorded in the access point's client table (association table). This recorded state has a size limit that can either be a hard-coded number or a number based on the physical memory constraint.

A form of DoS (denial-of-service) attack floods the access point's client state table (association table) by imitating many client stations (MAC address spoofing) sending authentication requests to the access point. Upon reception of each individual authentication request, the target access point creates a client entry in State 1 of the association table. If Open System authentication is used for the access point, the access point returns an *authentication success* frame and moves the client to State 2. If Shared-key authentication is used for the access point, the access point sends an *authentication challenge* to the attacker's imitated client which does not respond. In this case, the access point keeps the client in State 1. In either case, the access point contains multiple clients hanging in either State 1 or State 2 which fills up the access point association table. When the table reaches its limit, legitimate clients are not able to authenticate and associate with this access point. This results in a DoS attack.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form a DoS attack by tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security analyst can log on to the access point to check the current association table status.

Denial of Service Attack: EAPOL-Start Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP (Extensible Authentication Protocol) over LANs, or EAPOL. The 802.1x protocol starts with a EAPOL-Start frame sent by the client station to begin the authentication transaction. The access point responds to an EAPOL-Start frame with a EAP-Identity-Request and some internal resource allocation.

An attacker attempts to bring down an access point by flooding it with EAPOL-Start frames to exhaust the access point internal resources.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS (denial-of-service) attack by tracking the 802.1x authentication state transition and particular attack signature.

Denial of Service Attack: PS Poll Flood Attack

Alarm Description and Possible Causes

Power management is probably one of the most critical features of wireless LAN devices. Power management helps to conserve power by enabling stations to remain in power saving state mode for longer periods of time and to receive data from the access point only at specified intervals. The wireless client device must inform the access point of the length of time that it will be in the sleep mode (power save mode). At the end of the time period, the client wakes up and checks for waiting data frames. After it completes a handshake with the access point, it receives the data frames. The beacons from the access point also include the Delivery Traffic Indication Map (DTIM) to inform the client when it needs to wake up to accept multicast traffic.

The access point continues to buffer data frames for the sleeping wireless clients. Using the Traffic Indication Map (TIM), the access point notifies the wireless client that it has buffered data buffered. Multicast frames are sent after the beacon that announces the DTIM.

The client requests the delivery of the buffered frames using PS-Poll frames to the access point. For every PS-Poll frame, the access point responds with a data frame. If there are more frames buffered for the wireless client, the access point sets the data bit in the frame response. The client then sends another PS-Poll frame to get the next data frame. This process continues until all the buffered data frames are received.

A potential hacker could spoof the MAC address of the wireless client and send out a flood of PS-Poll frames. The access point then sends out the buffered data frames to the wireless client. In reality, the client could be in the power safe mode and would miss the data frames.

wIPS Solution

The Cisco Adaptive Wireless IPS can detect this DoS (denial-of-service) attack that can cause the wireless client to lose legitimate data. Locate the device and take appropriate steps to remove it from the wireless environment. Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing. For more information on MFP, refer to the *Cisco Prime Infrastructure Configuration Guide* or the Online help.

Denial of Service Attack: Probe Request Flood

Alarm Description and Possible Causes

A form of Denial of Service attack allows the attacker to force the target AP into a constant stream of wireless packets intended to serve nonexistent clients. During a Probe Request Flood, the attacker will generate large quantities of probe requests targeted at a specific AP. Typical wireless design specifies that an AP will respond to a probe request by sending a probe response, which contains information about the corporate network. Due to the volume of probe requests transmitted during a flood attack, the AP will be stuck continuously responding, thus resulting in a denial of service for all clients depending on that AP.

wIPS Solution

The wIPS server monitors the levels of probe request frames detected and will trigger a Probe Request Flood alarm when the threshold is exceeded. Even in cases where the requests are valid, the volume of the frames could cause problems with wireless activity. Consequently, the source(s) of the offending frames should be located and removed from the enterprise environment.

Denial of Service Attack: Re-association Request Flood

Alarm Description and Possible Causes

A form of Denial-of-service attack is to exhaust the AP's resources, particularly the client association table, by flooding the AP with a large number of emulated and spoofed client re-associations. At the 802.11 layer, Shared-key authentication is flawed and rarely used any more. The only 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 AP's client association table by creating many clients reaching State 3 as illustrated below. Once the client association table overflows, legitimate clients will not be able to get associated thus a denial-of-serve attack is committed.

wIPS Solution

The wIPS server monitors the levels of re-association requests on the network and triggers this alarm if the threshold is exceeded.

Denial of Service Attack: Unauthenticated Association

Alarm Description and 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 imitated 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 a higher level of authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker leveraging such a vulnerability can imitate 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 causing a DoS attack.

wIPS Solution

Denial of Service (DoS) attacks are unique in that most ways to contain them will not work. Unauthenticated Association Attack is no different. You have an attacker that is randomly generating hundreds if not thousands of MAC addresses and crafting those as Association frames and sending them as fast as possible to the target Access Point. Wireless containment on this type of attack is clearly not possible. What are your options?

Locating the source of the attack is your best option

- Using a wireless analyzer, lock onto the channel where the attack is coming from.

- Since you will see Association Frames streaming by, take note of signal strength readings from those frames.

- Using these signal strength numbers, try to locate the source of the attack by walking around the area where you think the attack is being generated from.

Denial of Service Attack Against Infrastructure

In addition to attacking access points or client stations, the wireless intruder may target the RF spectrum or the back-end authentication RADIUS server for DoS (denial of service) attacks. The RF spectrum can be easily disrupted by injecting RF noise generated by a high power antenna from a distance. Back-end RADIUS servers can be overloaded by a DDoS (distributed denial of service) attack where multiple wireless attackers flood the RADIUS server with authentication requests. This attack does not require a successful authentication to perform the attack.

DoS attacks against infrastructure include the following types:

Denial of Service Attack: Beacon Flood

Alarm Description and Possible Causes

A form of Denial of Service attack allows an attacker to inhibit wireless activity for the entire enterprise infrastructure by preventing new associations between valid APs and stations. Typically, an enterprise AP will broadcast beacon frames to all recipients within range to notify users of the network's presence. Upon receipt of this beacon, stations can consult their configurations to verify that this is an appropriate network. During a beacon flood attack, stations that are actively seeking a network are bombarded with beacons from networks generated using different MAC addresses and SSIDs. This flood can prevent the valid client from detecting the beacons sent by the corporate APs, and thus a denial of service attack is initiated.

wIPS Solution

The wIPS server monitors the levels of beacon frames detected and will trigger a Beacon Flood alarm when the threshold is exceeded. Even in cases where the beacons are valid, the volume of the frames could cause problems with wireless activity. Consequently, the sources of the offending frames should be located and removed from the enterprise environment.

Denial of Service Attack: CTS Flood

Attack tool: CTS Jack

Alarm Description and Possible Causes

As an optional feature, the IEEE 802.11 standard includes the RTS/CTS (Request-To-Send/Clear-To-Send) functionality to control the station access to the RF medium. The wireless device ready for transmission sends a RTS frame in order to acquire the right to the RF medium for a specified time duration. The receiver grants the right to the RF medium to the transmitter by sending a CTS frame of the same time duration. All wireless devices observing the CTS frame should yield the media to the transmitter for transmission without contention.

A wireless denial-of-service attacker may take advantage of the privilege granted to the CTS frame to reserve the RF medium for transmission. By transmitting back-to-back CTS frames, an attacker can force other wireless devices sharing the RF medium to hold back their transmission until the attacker stops transmitting the CTS frames.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the abuse of CTS frames for a DoS attack.

Denial of Service Attack: Destruction Attack

Alarm Description and Possible Causes

MDK3 is a suite of hacking tools that allows users to utilize a number of different security penetration methods against corporate infrastructures. MDK3-Destruction mode is a specific implementation of the suit that uses an array of the tools to effectively completely shut down a wireless deployment. During an MDK-Destruction attack, the tool simultaneously:

- Initiates a beacon flood attack, which creates fake APs within the environment,

- Triggers an authentication flood attack against valid corporate APs, preventing them from servicing clients, and kicks all active connections with valid clients.

Additional enhancements allow for the tool to be used to connect the valid clients to the fake APs generated with the beacon flood, causing further confusion in the environment.

wIPS Solution

The wIPS server monitors for the combination of symptoms of an MDK3-Destruction attack and triggers an alarm when they are detected. Due to the dramatic impact that this attack can have on a wireless deployment, it is strongly recommended that the source of the attack be identified and removed immediately in order to resume normal network operations.

Denial of Service Attack: Queensland University of Technology Exploit

Denial of Service Vulnerability in IEEE 802.11 Wireless Devices: US-CERT VU#106678 & Aus-CERT AA-2004.02

Alarm Description and Possible Causes

802.11 WLAN devices use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the basic access mechanism in which the WLAN device listens to the medium before starting any transmission and backs-off when it detects any existing transmission taking place. Collision avoidance combines the physical sensing mechanism and the virtual sense mechanism that includes the Network Allocation Vector (NAV), the time before which the medium is available for transmission. Clear Channel Assessment (CCA) in the DSSS protocol determines whether a WLAN channel is clear so an 802.11b device can transmit on it.

Mark Looi, Christian Wullems, Kevin Tham and Jason Smith from the Information Security Research Centre, Queensland University of Technology, Brisbane, Australia, have recently discovered a flaw in the 802.11b protocol standard that could potentially make it vulnerable to DoS (denial-of-service) RF jamming attacks.

This attack specifically attacks the CCA functionality. According to the AusCERT bulletin, "an attack against this vulnerability exploits the CCA function at the physical layer and causes all WLAN nodes within range, both clients and access points, to defer transmission of data for the duration of the attack. When under attack, the device behaves as if the channel is always busy, preventing the transmission of any data over the wireless network."

This DoS attack affects DSSS WLAN devices including IEEE 802.11, 802.11b, and low-speed (below 20Mbps) 802.11g wireless devices. IEEE 802.11a (using OFDM), high-speed (above 20Mbps using OFDM) 802.11g wireless devices are not affected by this attack. Devices that use FHSS are also not affected.

Any attacker using a PDA or a laptop equipped with a WLAN card can launch this attack on SOHO and enterprise WLANs. Switching to the 802.11a protocol is the only solution or known protection against this DoS attack.

For more information on this DoS attack refer to :

- http://www.auscert.org.au/render.html?it=4091

- http://www.qut.edu.au/institute-for-future-environments

- http://www.kb.cert.org/vuls/id/106678

wIPS Solution

The Cisco Adaptive Wireless IPS detects this DoS attack and sets off the alarm. Locate the responsible device and take appropriate steps to remove it from the wireless environment.

Denial of Service attack: RF Jamming Attack

Alarm Description and Possible Causes

Note   RF Jamming Attack is a channel alarm and does not contain alarm source or destination MAC address and hence no location will be generated for such alarms.

RF Jamming Attack does not populate attacker mac address. RF jamming is an attack against a particular channel. The attacker may send thousands of frames per second to jam the channel, and the frames are sent with different MAC addresses. Hence, you do not have a unique MAC address to identify the attacker.

WLAN reliability and efficiency depend on the quality of the RF media. Each RF is susceptible to RF noise impact. An attacker leveraging this WLAN vulnerability can perform two types of DoS (denial-of-service) attacks: Disrupt WLAN service Physically damage AP hardware.

- Disrupt WLAN service —At the 2.4GHz unlicensed spectrum, the attack may be unintentional. A cordless phone, Bluetooth devices, microwave, wireless surveillance video camera, or baby monitor can all emit RF energy to disrupt WLAN service. Malicious attacks can manipulate the RF power at 2.4GHz or 5GHz spectrum with a high gain directional antenna to amplify the attack impact from a distance. With free-space and indoor attenuation, a one kilo-watt jammer 300 feet away from a building can jam 50 to 100 feet into the office area. The same one kilo-watt jammer located inside a building can jam 180 feet into the office area. During the attack, WLAN devices in the target area are out of wireless service.

- Physically damage AP hardware— An attacker using a high output transmitter with directional high gain antenna 30 yards away from an access point can pulse enough high energy RF power to damage

electronics in the access point resulting in it being permanently out of service. Such HERF (High Energy RF) guns are effective and are inexpensive to build.

wIPS Solution

Like any RF based disturbance, your best way to resolve this would be to physically locate the device that is triggering the RF Jamming alarm and take it offline. Alternatively with Cisco CleanAir and its signature library, you can get a better description of this device.

- Find out the wIPS Access Point that triggered this alarm.

- Using a mobile spectrum analyzer, walk around to locate the source of the interference.

- Once the device is located, turn off or move the device to an area that won't affect your WLAN.

Denial of Service: RTS Flood

Alarm Description and Possible Causes

As an optional feature, the IEEE 802.11 standard includes the RTS/CTS (Request-To-Send/Clear-To-Send) functionality to control access to the RF medium by stations. The wireless device ready for transmission sends an RTS frame to acquire the right to the RF medium for a specified duration. The receiver grants the right to the RF medium to the transmitter by sending a CTS frame of the same duration. All wireless devices observing the CTS frame should yield the RF medium to the transmitter for transmission without contention.

A wireless denial of service attacker may take advantage of the privilege granted to the CTS frame to reserve the RF medium for transmission. By transmitting back-to-back RTS frames with a large transmission duration text box, an attacker reserves the wireless medium and force other wireless devices sharing the RF medium to hold back their transmissions.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the abuse of RTS frames for denial-of-service attacks.

Denial of Service Attack: Virtual Carrier Attack

Alarm Description and Possible Causes

The virtual carrier-sense attack is implemented by modifying the 802.11 MAC layer implementation to allow random duration values to be sent periodically. This attack can be carried out on the ACK, data, RTS, and CTS frame types by using large duration values. By doing this the attacker can prevent channel access to legitimate users. Under normal circumstances, the only time a ACK frame carries a large duration value is when the ACK is part of a fragmented packet sequence. A data frame legitimately carries a large duration value only when it is a subframe in a fragmented packet exchange.

One approach to deal with this attack is to place a limit on the duration values accepted by nodes. Any packet containing a larger duration value is truncated to the maximum allowed value. Low cap and high cap values can be used. The low cap has a value equal to the amount of time required to send an ACK frame, plus media access backoffs for that frame. The low cap is used when the only packet that can follow the observed packet

is an ACK or CTS. This includes RTS and all management (association, etc) frames. The high cap is used when it is valid for a data packet to follow the observed frame. The limit in this case needs to include the time required to send the largest data frame, plus the media access backoffs for that frame. The high cap must be used in two places: when observing an ACK (because the ACK my be part of a MAC level fragmented packet) and when observing a CTS.

A station that receives an RTS frame also receives the data frame. The IEEE 802.11 standard specifies the exact times for the subsequent CTS and data frames. The duration value of RTS is respected until the following data frame is received or not received. Either the observed CTS is unsolicited or the observing node is a hidden terminal. If this CTS is addressed to a valid in-range station, the valid station can nullify this by sending a zero duration null function frame. If this CTS is addressed to an out-of-range station, one method of defense is to introduce authenticated CTS frames containing cryptographically signed copies of the preceding RTS. With this method, there is a possibility of overhead and feasibility issues.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this DoS (denial-of-service) attack. Locate the device and take appropriate steps to remove it from the wireless environment.

Denial of Service Attacks Against Client Station

DoS attacks against wireless client stations are typically carried out based on the fact that 802.11 management frames and 802.1x authentication protocols have no encryption mechanism and thus can be spoofed. For example, wireless intruders can disrupt the service to a client station by continuously spoofing a 802.11 disassociation or deauthentication frame from the access point to the client station.

Besides the 802.11 authentication and association state attack, there are similar attack scenarios for 802.1x authentication. For example, 802.1x EAP-Failure or EAP-logoff messages are not encrypted and can be spoofed to disrupt the 802.1x authenticated state to disrupt wireless service.

Cisco Adaptive Wireless IPS tracks the client authentication process and identifies DoS attack signatures. Incomplete authentication and association transactions trigger the attack detection and statistical signature matching process. Detected DoS attack results in setting off wIPS alarms that include the usual alarm detail description and target device information.

DoS attacks against client station include the following types:

Denial of Service Attack: Authentication Failure Attack

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this client state machine based on the IEEE standard (see illustration below). A successfully associated client station remains in State 3 in order to continue wireless communication. A client station in State 1 and in State 2 cannot participate in the WLAN data communication process until it is authenticated and associated to State 3. IEEE 802.11 defines two authentication services: Open System Authentication and Shared Key Authentication. Wireless clients go through one of these authentication processes to associate with an access point.

A denial-of-service (DoS) attack spoofs invalid authentication request frames (with bad authentication service and status codes) from an associated client in State 3 to an access point. Upon reception of the invalid authentication requests, the access point updates the client to State 1, which disconnects its wireless service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of a DoS attack by monitoring for spoofed MAC addresses and authentication failures. This alarm may also indicate an intrusion attempt. When a wireless client fails too many times in authenticating with an access point, the server raises this alarm to indicate a potential intruder's attempt to breach security.

> **Note** This alarm focuses on 802.11 authentication methods, such as Open System and Shared Key. 802.1x and EAP based authentications are monitored by other alarms.

Denial of Service Attack: Block ACK Flood

Alarm Description and Possible Causes

A form of Denial of Service attack allows an attacker to prevent an 802.11n AP from receiving frames from a specific valid corporate client. With the introduction of the 802.11n standard, a transaction mechanism was introduced which allows a client to transmit a large block of frames at once, rather than dividing them up into segments. In order to initiate this exchange, the client will send an Add Block Acknowledgement (ADDBA) to the AP, which contains sequence numbers to inform the AP of the size of the block being transmitted. The AP will then accept all frames that fall within the specified sequence (consequently dropping any frames that fall outside of the range) and transmit a BlockACK message back to the client when the transaction has been completed.

In order to exploit this process, an attacker can transmit an invalid ADDBA frame while spoofing the valid client's MAC address. This process will cause the AP to ignore any valid traffic transmitted from the client until the invalid frame range has been reached.

wIPS Solution

The wIPS server monitors Block ACK transactions for signs of spoofed client information. When an attacker is detected attempting to initiate a Block ACK attack, an alarm is triggered. It is recommended that users locate the offending device and eliminate it from the wireless environment as soon as possible.

Denial of Service Attack: Deauthentication Broadcast

Attack tool: WLAN Jack, Void11, Hunter Killer

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client station remains in State 3 to continue wireless communication. A client station in State 1

and State 2 can not participate in WLAN data communication until it is authenticated and associated to State 3.

A form of DoS (denial-of-service) attack aims to send all clients of an access point to the unassociated or unauthenticated State 1 by spoofing de-authentication frames from the access point to the broadcast address. With today's client adapter implementation, this form of attack is very effective and immediate in terms of disrupting wireless services against multiple clients. Typically, client stations re-associate and re-authenticate to regain service until the attacker sends another de-authentication frame.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed de-authentication frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security analyst can log on to the access point to check the current association table status.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the Cisco Prime Infrastructure Configuration Guide or Online help.

Denial of Service Attack: Deauthentication Flood

Attack tool: WLAN Jack, Void11

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client station stays in State 3 in order to continue wireless communication. A client station in State 1 and State 2 can not participate in WLAN data communication until it is authenticated and associated to State 3.

A form of DoS (denial-of-service) attack aims to send an access point's client to the unassociated or unauthenticated State 1 by spoofing de-authentication frames from the access point to the client unicast address. With today's client adapter implementations, this form of attack is very effective and immediate in terms of disrupting wireless services against the client. Typically, client stations re-associate and re-authenticate to regain service until the attacker sends another de-authentication frame. An attacker repeatedly spoofs the de-authentication frames to keep all clients out of service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed dis-association frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log on to the access point to check the current association table status.

Denial of Service Attack: Disassociation Flood

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client station stays in State 3 in order to continue wireless communication. A client station in State 1 and State 2 can not participate in WLAN data communication until it is authenticated and associated to State 3.

A form of DoS (denial-of-service) attack aims to send an access point's client to the unassociated or unauthenticated State 2 by spoofing dis-association frames from the access point to the broadcast address (all clients). With today's client adapter implementations, this form of attack is effective and immediate in terms of disrupting wireless services against multiple clients. Typically, client stations re-associate to regain service until the attacker sends another dis-association frame. An attacker repeatedly spoofs the dis-association frames to keep all clients out of service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed dis-association frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log on to the access point to check the current association table status.

Denial of Service Attack: EAPOL Logoff Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP (Extensible Authentication Protocol) over LANs, or EAPOL. The 802.1x protocol starts with a EAPOL-Start frame to begin the authentication transaction. At the end of an authenticated session when a client station wishes to log off, the client station sends an 802.1x EAPOL-Logoff frame to terminate the session with the access point.

Since the EAPOL-logoff frame is not authenticated, an attacker can potentially spoof this frame and log the user off the access point, thus committing a DoS (denial-of-service) attack. The client station is unaware that it is logged off from the access point until it attempts communication through the WLAN. Typically, the client station discovers the disrupted connection status and re-associates and authenticates automatically to regain the wireless connection. The attacker can continuously transmit the spoofed EAPOL-Logoff frames to be effective on this attack.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the use of FATA-jack by monitoring on spoofed MAC addresses and authentication failures. This alarm may also indicate an intrusion attempt. When a wireless client fails too many times in authenticating with an access point, the Cisco Adaptive Wireless IPS raises this alarm to indicate a potential intruder's attempt to breach security.

Note This alarm focuses on 802.11 authentication methods (Open System, Shared Key, etc). EAP and 802.1x based authentications are monitored by other alarms.

Denial of Service Attack: FATA Jack Tool Detected

Alarm Description and Possible Causes

EEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this state machine based on the IEEE standard. A successfully associated client station stays in State 3 in order to continue wireless communication. A client station in State 1 and in State 2 cannot participate in the WLAN data communication process until it is authenticated and associated to State 3. IEEE 802.11 defines two authentication services: Open System Authentication and Shared Key Authentication. Wireless clients go through one of these authentication processes to associate with an access point.

A form of DoS (denial-of-service) attack spoofs invalid authentication request frames (with bad authentication service and status codes) from an associated client in State 3 to an access point. Upon reception of the invalid authentication requests, the access point updates the client to State 1, which disconnects its wireless service.

FATA-jack is one of the commonly used tools to run a similar attack. It is a modified version of WLAN-jack and it sends authentication-failed packets along with the reason code of the previous authentication failure to the wireless station. This occurs after it spoofs the MAC address of the access point. FATA-jack closes most active connections and at times forces the user to reboot the station to continue normal activities.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking the spoofed pre-mature EAP-Failure frames and the 802.1x authentication states for each client station and access point. Locate the device and take appropriate steps to remove it from the wireless environment.

Denial of Service Attack: Premature EAP Failure Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP (Extensible Authentication Protocol) over LANs, or EAPOL. The 802.1x protocol starts with a EAPOL-Start frame to begin the authentication transaction. When the 802.1x authentication packet exchange is complete with the back-end RADIUS server, the access point sends an EAP-Success or EAP-Failure frame to the client to indicate authentication success or failure.

The IEEE 802.1X specification prohibits a client from displaying its interface when the required mutual authentication is not complete. This enables a well-implemented 802.1x client station to avoid being fooled by a fake access point sending premature EAP-Success packets.

An attacker keeps the client interface from displaying (therefore Denial-of-Service) by continuously spoofing pre-mature EAP-Failure frames from the access point to the client to disrupt the authentication state on the client.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking spoofed premature EAP-Success frames and the 802.1x authentication states for each client station and access point. Locate the device and take appropriate steps to remove it from the wireless environment.

Intrusion Detection—Security Penetration

A form of wireless intrusion is to breach the WLAN authentication mechanism to gain access to the wired network or the wireless devices. Dictionary attacks on the authentication method is a common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked access point attack on a unsuspicious wireless client may fool the client into associating with faked access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.

These security threats can be prevented if mutual authentication and strong encryption techniques are used. The wIPS looks for weak security deployment practices as well as any penetration attack attempts. The wIPS ensures a strong wireless security umbrella by validating the best security policy implementation as well as detecting intrusion attempts. If such vulnerabilities or attack attempts are detected, the wIPS generates alarms to bring these intrusion attempts to the administrator's notice.

Security penetration attacks include the following types:

ASLEAP Tool Detected

Alarm Description and Possible Causes

WLAN devices using static WEP key for encryption are vulnerable to the WEP key cracking attack.

Cisco Systems introduced LEAP (Lightweight Extensible Authentication Protocol) to leverage the existing 802.1x framework to avoid such WEP key attacks. The Cisco LEAP solution provides mutual authentication, dynamic per session and per user keys, and configurable WEP session key time out. The LEAP solution was considered a stable security solution and is easy to configure.

There are hacking tools that compromise wireless LAN networks running LEAP by using off-line dictionary attacks to break LEAP passwords After detecting WLAN networks that use LEAP, this tool de-authenticates users which forces them to reconnect and provide their user name and password credentials. The hacker captures packets of legitimate users trying to re-access the network. The attacker can then analyze the traffic off-line and guess the password by testing values from a dictionary.

The main features of the ASLEAP tool include:

- Reading live from any wireless interface in RFMON mode with libpcap
- Monitoring a single channel or performing channel hopping to look for target networks running LEAP.
- Actively deauthenticating users on LEAP networks, forcing them to reauthenticate. This allows quick LEAP password captures.
- Only de-authenticating users who have not already been seen rather than users who are not running LEAP.

- Reading from stored libpcap files.

- Using a dynamic database table and index to allow quick lookups on large files. This reduces the worst-case search time to .0015% as opposed to lookups in a flat file.

- Writing only the LEAP exchange information to a libpcap file.

This could be used to capture LEAP credentials with a device short on disk space (like an iPaq); the LEAP credentials are then stored in the libpcap file on a system with more storage resources to mount the dictionary attack.

The source and Win32 binary distribution for the tool are available at http://asleap.sourceforge.net.

Cisco Systems has developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol which stops these dictionary attacks. EAP-FAST helps prevent man-in-the-middle attacks, dictionary attacks, and packet and authentication forgery attacks. In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is then authenticated using the user-name and password credentials.

Some advantages of EAP-FAST include:

- It is not proprietary.

- It is compliant with the IEEE 802.11i standard.

- It supports TKIP and WPA.

- It does not use certificates and avoids complex PKI infrastructures.

- It supports multiple Operating Systems on PCs and Pocket PCs.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the de-authentication signature of the ASLEAP tool. Once detected, the server alerts the wireless administrator. The user of the attacked station should reset the password. The best solution to counter the ASLEAP tool is to replace LEAP with EAP-FAST in the corporate WLAN environment.

Cisco WCS also provides automated security vulnerability scanning that proactively reports any access points configured to utilize weak encryption or authentication. For more information on automated security vulnerability scanning, refer to Cisco WCS online help.

Airdrop Session Detected

Alarm and Possible Causes

Starting with Apple OSX Lion, Apple has a new feature called AirDrop. This new feature is supported on "newer" MacBook, MacBook Pro and iMac. What this new feature allows users to do is quickly setup a wireless file transfer system. To achieve this, both of the users that want to share files need to open their finder and click on the AirDrop link. Once both of the systems are in range of each other and the link is setup, the users will see the other user's login icon in the AirDrop window. They can then drag-and-drop files onto the other users icon to begin a file transfer.

This could potentially create a security risk due to unauthorized Peer-to-Peer networks being dynamically created in your WLAN environment. File sharing is also a concern here.

wIPS Solution

The system monitors the wireless network for traffic consistent with an AirDrop session. Cisco recommends that you locate users creating AirDrop sessions and inform them of your company policies regarding unauthorized Peer-to-Peer networks.

AirPwn

Alarm Description and Possible Causes

Airpwn is a framework for 802.11 packet injection. Airpwn listens to incoming wireless packets, and if the data matches a pattern specified in the config files, custom content is injected (spoofed) from the wireless access point. Airpwn utilizes the inherent delay when a client sends a request to the internet. Since the Airpwn attacker is closer, it will be able to quickly respond. As an example, the hacker might replace all images on a website that the visitor is trying to view, showing only what the hacker wants the visitor to see.

Airpwn only works on open wireless networks and WEP encrypted networks when the attacker knows the WEP key.

wIPS Solution

Cisco Enterprise monitors the wireless network for potential traffic that is consistent with an Airpwn attack against Open or WEP decrypted Access Points and notifies the WLAN administrator. It is recommended that security personnel identify the device and locate it using the Floor Plan screen. The attacking station should be removed from the wireless environment as soon as possible.

Airsnarf Attack Detected

Alarm Description and Possible Causes

wIPS Solution

The Cisco Adaptive Wireless IPS detects the wireless device running the AirSnarf tool. Appropriate action must be taken by the administrator to remove the AirSnarf tool from the WLAN environment.

Bad EAP-TLS Frames

Alarm Description and Possible Causes

Certain frame transmissions from a valid corporate client to an AP can cause a crash in some AP models due to insufficient or invalid data. A wireless attacker can take advantage of this vulnerability by transmitting the defective frames in order to bring down a corporate AP. By sending EAP-TLS packets with flags set to 'c0' and no TLS message length or data, APs from some vendors can be rendered inoperable until they are rebooted. During this reboot process, attackers may have a brief opportunity to gain access to the corporate network, resulting in a potential security leak.

wIPS Solution

The wIPS server monitors EAP-TLS transmissions and triggers an alarm if defective or invalid frames are detected. Although this issue may not always represent a wireless attack, it is an issue that should be remedied in order to maintain the health of the overall wireless deployment.

Beacon Fuzzed Frame Detected

Alarm Description and Possible Causes

802.11 Fuzzing is the process of introducing invalid, unexpected or random data into the 802.11 frames and then replaying those modified frames into the air. This can cause unexpected behavior to the destination device including driver crashes, operating system crashes and stack based overflows which would allow execution of arbitrary code on the affected system. The CVE website (http://cve.mitre.org/index.html) has numerous reported entries for fuzzing based vulnerabilities on 802.11 frames.

The system inspects each beacon frame looking for signs of fuzzing activity. Most common forms of beacon fuzzing involve expanding the SSID field beyond the limit of 32 bytes and changing the supported data rates to invalid rates. The system looks for these anomalies and will generate the Beacon Fuzzing alarm when the field values are beyond the 802.11 specification.

wIPS Solution

The system monitors the wireless network for traffic consistent with Beacon Fuzzing. It is recommended to locate the device and take it offline.

Brute Force Hidden SSID

Alarm Description and Possible Causes

A common practice amongst WLAN Administrators is to disable broadcasting of the SSID for an Access Point. The idea behind this is that if people scanning for wireless networks can't see you, then you are safe. Basically you would need to know the SSID in order to connect to that wireless network. This protects your

wireless network from casual drive by users who don't have the tools to extract the SSID from hidden networks. But hackers are a different story. They have the tools, the time and energy to extract the SSID from hidden networks. There are many tools to perform this type of snooping. If a hidden SSID is not found through normal methods, hackers can use a brute force method using the tool mdk3. With the tool mdk3, they can perform a Dictionary attack or a word list attack on the hidden network to extract the SSID.

wIPS Solution

Cisco Enterprise monitors the wireless network for potential traffic that is consistent with a brute force attack against a hidden SSID and notifies the WLAN administrator. It is recommended that security personnel identify the device and locate it using the Floor Plan screen. The attacking station should be removed from the wireless environment as soon as possible.

ChopChop Attack

Alarm Description and Possible Causes

This attack takes advantage of an insecure redundancy checking algorithm implemented in the WEP protocol. By compromising a few known properties, an attacker is able to take an encrypted packet and decrypt it while retrieving the keystream used to encrypt the packet.

The way the attack works, is the attacker captures a packet and chops one byte off the end of the packet before the ICV.

The attacker will then append a "guess" to the decrypted value of the byte. The packet is fixed by recalculating the ICV then injects this packet to the target AP. If the target AP, re-broadcasts this frame back out, the attacker knows he has correctly guessed the value of the decrypted byte. The attacker then moves onto the next byte. As the guesses become successful, the packet being injected actually gets smaller and smaller. If the packet doesn't get re-broadcasted, then the attacker changes the guess and repeats the process, he or she has 256 possible choices to try and guess. Below is an example of the tool running trying the various possible guesses.

Once complete, the attacker will have decrypted the entire WEP packet byte by byte, which can then be XORed with the original encrypted packet to produce the plaintext data.

wIPS Solution

The ChopChop Attack is targeted at WEP based Access Points to break the WEP key and gain direct access to the wireless network. Since this particular attack can take less than 5 minutes to perform, there is a good chance the attacker has already gained access to your wireless network. If possible, migrate your WLAN off WEP. WPA2-AES is recommended. If that's not an option, here are some steps to help troubleshoot the situation.

- Turn off the radios for the affected AP. This will disconnect all clients that are currently connected.
- Change the WEP key
- Turn the radios back on
- You will need to change the WEP key on all of the devices that were currently connected to the new WEP key that was just set.
- Monitor NCS to see if the ChopChop alarm happens again.

DHCP Starvation Attack Detected (ID:215)

Alarm Description and Possible Causes

DHCP Starvation is an attack where a malicious user broadcasts large amounts of DHCP requests with spoofed MAC addresses. If enough DHCP request frames flood the network, the attacker could use up all of the remaining DHCP IP addresses that are available for valid users. This would create a DoS condition on the network. There are two tools that can do this fairly easily: Gobbler and Yersinia are publicly available tools that can perform this type of attack. This type of attack is especially harmful on guest networks or hotspot networks where the user is allowed to get an IP address before the authentication happens.

Mitigation options for this type of attack can be handled at the switch level. For Cisco IOS switches, enable DHCP Snooping. For Cisco CatOS, enable port security.

wIPS Solution

The system monitors the wireless network for traffic consistent with a DHCP Starvation attack. Cisco recommends that you locate the user running the attack or implement tighter switch security.

Day-0 Attack by WLAN Security Anomaly

wIPS Solution

The Cisco Adaptive Wireless IPS has detected a single Security IDS/IPS policy violation on a large number of devices in the wireless network. Either the number of devices violating the specific policy in the time period specified are observed or there is a sudden percentage increase in the number of devices as specified in the threshold settings for the alarm. Depending on the Security IDS/IPS violation, it is suggested that the violation be monitored individually to determine the source and destination of this attack. If this is an increase in the number of rogue devices, it may indicate an attack against the network.

If there is a sudden increase in the number of client devices with encryption disabled, it may be necessary to revisit the Corporate Security Policy and enforce users to use the highest level of encryption and authentication according to the policy rules.

Day-0 Attack by Device Security Anomaly

wIPS Solution

The Cisco Adaptive Wireless IPS detects a device violating a large number of Security IDS/IPS policies. This device has either generated a number of Security IDS/IPS violations in the time period specified or there is a sudden percentage increase as specified in the threshold settings for the various alarms. The device should be monitored and located to carry out further analysis to check if this device is compromising the Enterprise Wireless Network in any way (attack or vulnerability). If this is a rogue device, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find it.

Device Broadcasting XSS SSID

Alarm Description and Possible Causes

Cross-Site scripting vulnerabilities are well known and consist of publicized attacks that target web applications to gain access to the underlying server or the web application itself. It does this by injecting a client-side script into web pages viewed by the user.

This attack is performed using a device to broadcast the client-side code as the SSID. Once a WLAN monitoring system picks up the malicious SSID and records it, if the system is web based and there are Cross-Site Scripting vulnerabilities, then that system will be exploited once the device with the malicious SSID is clicked.

wIPS Solution

Cisco Enterprise monitors the wireless network for Access Points and Ad-hoc devices broadcasting malicious Cross-site scripting (XSS) traffic. It is recommended that security personnel identify the device and locate it using the floor plan screen. The device should then be removed from the wireless environment as soon as possible.

Device Probing for Access Points

Some commonly used scan tools include: NetStumbler (newer versions), MiniStumbler (newer versions), MACStumbler, WaveStumbler, PrismStumbler, dStumbler, iStumbler, Aerosol, Boingo Scans, WiNc, AP Hopper, NetChaser, Microsoft Windows XP scans.

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects wireless devices probing the WLAN and attempting association (i.e. association request for an access point with any SSID).

Such devices could pose potential security threats in one of the following ways:

- War-driving, WiLDing (Wireless LAN Discovery), war-chalking, war-walking, war cycling, war-lightrailing, war-busing, and war-flying.

- Legitimate wireless client attempting risky promiscuous association.

War-driving, war-chalking, war-walking, and war-flying activities include:

- War-driving- A wireless hacker uses war-driving tools to discover access points and publishes information such as MAC address, SSID, and security implemented on the Internet with the access points' geographical location information.

- War-chalking- War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols

- War-flying-War-flying refers to sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet relay chat sessions from an altitude of 1,500 feet on a war-flying trip.

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your the access points to not broadcast SSIDs. Use the Cisco Adaptive Wireless IPS to see which access points are broadcasting (announcing) their SSID in the beacons.

Dictionary Attack on EAP Methods

Alarm Description and Possible Causes

IEEE 802.1x provides an EAP (Extensible Authentication Protocol) framework for wired or wireless LAN authentication. An EAP framework allows flexible authentication protocol implementation. Some implementations of 802.1x or WPA use authentication protocols such as LEAP, MD5, OTP (one-time-password), TLS, and TTLS. Some of these authentication protocols are based upon the user name and password mechanism, where the user name is transmitted clear without encryption and the password is used to answer authentication challenges.

Most password-based authentication algorithms are susceptible to dictionary attacks. During a dictionary attack, an attacker gains the user name from the unencrypted 802.1x identifier protocol exchange. The attacker then tries to guess a user's password to gain network access by using every "word" in a dictionary of common passwords or possible combinations of passwords. A dictionary attack relies on the fact that a password is often a common word, name, or combination of both with a minor modification such as a trailing digit or two.

A dictionary attack can take place actively online, where an attacker repeatedly tries all the possible password combinations. Online dictionary attacks can be prevented using lock-out mechanisms available on the authentication server (RADIUS servers) to lock out the user after a certain number of invalid login attempts. A dictionary attack can also take place off-line, where an attacker captures a successful authentication challenge protocol exchange and then tries to match the challenge response with all possible password combinations off-line. Unlike online attacks, off-line attacks are not easily detected. Using a strong password policy and periodically expiring user passwords significantly reduces an off-line attack tool's success.

wIPS Solution

The Cisco Adaptive Wireless IPS detects online dictionary attacks by tracking 802.1x authentication protocol exchange and the user identifier usages. Upon detection of a dictionary attack, the alarm message identifies the user name and attacking station's MAC address.

The Cisco Adaptive Wireless IPS advises switching user name and password based authentication methods to encrypted tunnel based authentication methods such as PEAP and EAP-FAST, which are supported by many vendors including Cisco.

Fake Access Points Detected

Alarm Description and Possible Causes

The Fake AP tool is meant to protect your WLAN acting as a decoy to confuse war-drivers using NetStumbler, Wellenreiter, MiniStumbler, Kismet, etc. The tool generates beacon frames imitating thousands of counterfeit 802.11b access points. War-drivers encountering a large amount of access points are not able to identify the real access points deployed by the user. This tool, although very effective in fending off war-drivers, poses other disadvantages such as bandwidth consumption, misleading legitimate client stations, and interference with the WLAN management tools. The Cisco Adaptive Wireless IPS does not recommend running the Fake AP tool in your WLAN.

wIPS Solution

The Cisco Adaptive Wireless IPS recommends that the administrator locate the device running the Fake AP tool and take appropriate steps to remove it from the wireless environment.

Fake DHCP Server Detected

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects such wireless STAs running the DHCP service and providing IP addresses to unaware users.

Once the client is identified and reported, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the device.

wIPS Solution

The Cisco Adaptive Wireless IPS detects such wireless STAs running the DHCP service and providing IP addresses to unaware users.

Once the client is identified and reported, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the device.

Fast WEP Crack (ARP Replay) Detected

Alarm Description and Possible Causes

It is well publicized that WLAN devices using static WEP key for encryption are vulnerable to WEP key cracking attack (Refer to Weaknesses in the Key Scheduling Algorithm of RC4 - I by Scott Fluhrer, Itsik Mantin, and Adi Shamir).

The WEP secret key that has been cracked by any intruder results in no encryption protection, thus leading to compromised data privacy. The WEP key that is in most cases 64-bit or 128-bit (few vendors also offer 152-bit encryption) consists of the secret key specified by the user linked with the 24-bit IV (Initialization Vector). The IV that is determined by the transmitting station can be reused frequently or in consecutive frames, thus increasing the possibility of the secret key to be recovered by wireless intruders.

The most important factor in any attack against the WEP key is the key size. For 64-bit WEP keys, around 150K unique IVs and for 128-bit WEP keys around 500k to a million unique IVs should be enough. With insufficient traffic, hackers have created a unique way of generating sufficient traffic to perform such an attack. This is called the replay attack based on arp-request packets. Such packets have a fixed length and can be spotted easily. By capturing one legitimate arp-request packet and resending them repeatedly, the other host responds with encrypted replies, providing new and possibly weak IVs.

wIPS Solution

The Cisco Adaptive Wireless IPS alerts on weak WEP implementations and recommends a device firmware upgrade if available from the device vendor to correct the IV usage problem. Ideally, enterprise WLAN networks can protect against WEP vulnerability by using the TKIP (Temporal Key Integrity Protocol) encryption mechanism, which is now supported by most enterprise level wireless equipment. TKIP enabled devices are not subject to any such WEP key attacks.

Cisco WCS also provides automated security vulnerability scanning that proactively reports any access points configured to utilize weak encryption or authentication. For more information on automated security vulnerability scanning, refer to the Cisco WCS online help.

Fragmentation Attack

Alarm Description and Possible Causes

It is well publicized that a WLAN device using a static WEP key for encryption is vulnerable to various WEP cracking attacks. Refer to Weaknesses in the Key Scheduling Algorithm of RC4 - I, by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information.

wIPS Solution

The Cisco Adaptive Wireless IPS alerts on detecting a potential fragmentation attack in progress, and recommends that WEP not be used in the corporate environment and that appropriate measures be taken to avoid any security holes in the network and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard.

HT Intolerant Degradation Services

Alarm Description and Possible Causes

While 802.11n deployments provide the potential for dramatically increased wireless range and speed over legacy implementations, these benefits can be easily lost or offset if a single legacy device is introduced to the network. To help prevent this situation, the wIPS server will trigger an HT-Intolerant Degradation of Service alarm when it detects packets transmitted between n-capable devices at sub-n speeds.

Alarm Description and Possible Causes

While 802.11n deployments provide the potential for dramatically increased wireless range and speed over legacy implementations, these benefits can be easily lost or offset if a single legacy device is introduced to the network. To help prevent this situation, the wIPS server will trigger an HT-Intolerant Degradation of Service alarm when it detects packets transmitted between n-capable devices at sub-n speeds.

Honeypot AP Detected

Alarm Description and Possible Causes

The addition of WLANs in the corporate environment introduces a whole new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured access points, unconfigured access points, and DoS (denial-of-service) attacks.

One of the most effective attacks facing enterprise networks implementing wireless is the use of a "honey pot" access point. An intruder uses tools such as NetStumbler, Wellenreiter, and MiniStumbler to discover the SSID of the corporate access point. Then the intruder sets up an access point outside the building premises or, if possible, within the premises and broadcasts the discovered corporate SSID. An unsuspecting client then connects to this "honey pot" access point with a higher signal strength. Once associated, the intruder performs attacks against the client station because traffic is diverted through the "honey pot" access point.

wIPS Solution

Once a "honey pot" access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

Hot-Spotter Tool Detected (Potential Wireless Phishing)

Alarm Description and Possible Causes

A hotspot is any location where Wi-Fi network access available for the general public. Hotspots are often found in airports, hotels, coffee shops, and other places where business people tend to congregate. It is currently one of the most important network access service for business travelers. The customer requires a wireless-enabled laptop or handheld to connect to the legitimate access point and to receive service. Most hotspots do not require the user to have an advanced authentication mechanism to connect to the access point, other than using a web page to log in. The criterion for entry is only dependent on whether or not the subscriber has paid subscription fees. In a wireless hotspot environment, no one should trust anyone else. Due to current security concerns, some WLAN hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user.

The four components of a basic hotspot network are:

- Hotspot Subscribers-Valid users with a wireless enabled laptop or handheld and valid login for accessing the hotspot network.

- WLAN Access Points-SOHO gateways or enterprise level access points depending upon the hotspot implementation.

- Hotspot Controllers-Deals with user authentication, gathering billing information, tracking usage time, filtering functions, etc. This can be an independent machine or can be incorporated in the access point itself.

- Authentication Server-Contains the login credentials for the subscribers. In most cases, hotspot controllers verify subscribers' credentials with the authentication server.

Hotspotter automates a method of penetration against wireless clients, independent of the encryption mechanism used. Using the Hotspotter tool, the intruder can passively monitors the wireless network for probe request frames to identify the SSIDs of the networks of the Windows XP clients.

After it acquires the preferred network information, the intruder compares the network name (SSID) to a supplied list of commonly used hotspot network names. Once a match is found, the Hotspotter client acts as an access point. The clients then authenticate and associate unknowingly to this fake access point.

Once the client gets associated, the Hotspotter tool can be configured to run a command such as a script to kick off a DHCP daemon and other scanning against the new victim.

Clients are also susceptible to this kind of attack when they are operating in different environments (home and office) while they are still configured to include the hotspot SSID in the Windows XP wireless connection settings. The clients send out probe requests using that SSID and make themselves vulnerable to the tool.

wIPS Solution

Once the rogue access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

Identical Send and Receive Address

Alarm Description and Possible Causes

In order to inhibit wireless activity in a corporate network, attackers will often modify wireless packets to emulate various different characteristics, including changes to the packets' Source and Destination MAC information. In cases where these fields are identical, the Identical Send and Receive Address alarm will be triggered in order to alert IT personnel of a potential attack.

wIPS Solution

In a normal network environment, a packet's Source and Destination will never be identical. As such, the enterprise administrators should take immediate steps to locate the root cause of the modified packets.

Improper Broadcast Frames

Alarm Description and Possible Causes

Standard 802.11 deployments allow for certain frames to be transmitted to individual destinations (also known as unicast frames, such as an ACK) and other frames to be 'broadcast' to all recipients in the wireless deployment. In general, these two categories should not overlap, e.g., an Association Request frame should not be sent out as a broadcast to all listening devices. In this scenario, the wIPS server will trigger an Improper Broadcast Frames alarm to alert staff of a potential problem.

Improper Broadcast Frames

Karma Tool Detected

Alarm Description and Possible Causes

The Karma tool allows a wireless attacker to configure a client as a soft AP that will respond to any probe request detected. This implementation is designed to respond to queries from stations configured to connect to multiple different networks, e.g., SSID "Corporate" for work and SSID "Home" for home use. In this example, the soft AP may be configured to respond to the probe for "Home" when the client is at work. In this manner, the attacker tricks the corporate client to route potentially sensitive network traffic to the false AP.

wIPS Solution

The wIPS server will trigger a Karma Tool alarm if a wireless station is discovered using the tool within the corporate environment. Users should locate the attacking device and eliminate it immediately.

Man-in-the-Middle Attack Detected

Alarm Description and Possible Causes

Man-in-the-Middle (MITM) attack is one of the most common 802.11 attacks that can lead to confidential corporate and private information being leaked to hackers. In a MITM attack, the hacker can use a 802.11 wireless analyzer and monitor 802.11 frames sent over the WLAN. By capturing the wireless frames during the association phase, the hacker gets IP and MAC address information about the wireless client card and access point, association ID for the client, and the SSID of the wireless network.

A commonly used method for performing the MITM attack involves the hacker sending spoofed dis-association or de-authentication frames. The hacker station then spoofs the MAC address of the client to continue an association with the access point. At the same time, the hacker sets up a spoofed access point in another channel to keep the client associated. This allows all traffic between the valid client and access point to pass through the hacker's station.

One of the most commonly used MITM attack tools is Monkey-Jack.

wIPS Solution

The Cisco Adaptive Wireless IPS recommends the use of strong encryption and authentication mechanisms to thwart any MITM attacks by hackers. One way to avoid such an attack is to prevent MAC spoofing by using MAC address exclusion lists and monitoring the RF channel environment.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MITM attacks. For more information on MFP, refer to the Cisco Wireless Control System Configuration Guide or the WCS online help.

NetStumbler Detected

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (such as an association request for an access point with any SSID) using the NetStumbler tool. The Device probing for Access Point alarm is generated when hackers use recent versions of the NetStumbler tool. For older versions, the Cisco Adaptive Wireless IPS generates the NetStumbler detected alarm.

NetStumbler is the most widely used tool for war-driving and war-chalking. A wireless hacker uses war-driving tools to discover access points and to publish their information (MAC address, SSID, security implemented, etc.) on the Internet with the access points' geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similiar to war-driving, but the hacker is on foot instead of a car. It can run on a machine running Windows 2000, Windows XP, or better. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up email and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which of your access points is broadcasting an SSID in the beacons.

Cisco WCS also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, refer to the WCS online help.

NetStumbler Victim Detected

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which access point is broadcasting its SSID in the beacons.

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (i.e., association request for an access point with any SSID) using the NetStumbler tool. The Device probing for access point alarm is generated when hackers more recent versions of the NetStumbler tool. For older versions, the Cisco Adaptive Wireless IPS generates the NetStumbler detected alarm.

NetStumbler is the most widely used tool for war-driving, war-walking, and war-chalking. A wireless hacker uses war-driving tools to discover access points and publish their information (MAC address, SSID, security implemented, etc.) on the Internet with the access points' geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similar to war-driving, but the hacker conducts the illegal operation on foot instead of by car. The NetStumbler web site (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or later. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers typically use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used, but from a low-flying private plane with high-power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.

The Cisco Adaptive Wireless IPS alerts the user when it observes that a station running Netstumbler is associated to a corporate access point.

Publicly Secure Packet Forwarding (PSPF) Violation

Alarm Description and Possible Causes

Publicly Secure Packet Forwarding (PSPF) is a feature implemented on WLAN access points to block wireless clients from communicating with other wireless clients. With PSPF enabled, client devices cannot communicate with other client devices on the wireless network.

For most WLAN environments, wireless clients communicate only with devices such as web servers on the wired network. By enabling PSPF it protects wireless clients from being hacked by a wireless intruder. PSPF is effective in protecting wireless clients especially at wireless public networks (hotspots) such as airports, hotels, coffee shops, and college campuses where authentication is null and anyone can associate with the access points. The PSPF feature prevents client devices from inadvertently sharing files with other client devices on the wireless network.

wIPS Solution

The Cisco Adaptive Wireless IPS detects PSPF violations. If a wireless client attempts to communicate with another wireless client, the Cisco Adaptive Wireless IPS raises an alarm for a potential intrusion attack. This alarm does not apply if your WLAN deploys wireless printers or VoWLAN applications because these applications rely on wireless client-to-client communication

Probe Request Fuzzed Frame Detected

Alarm Description and Possible Causes

802.11 Fuzzing is the process of introducing invalid, unexpected or random data into the 802.11 frames and then replaying those modified frames into the air. This can cause unexpected behavior to the destination device including driver crashes, operating system crashes and stack based overflows which would allow execution of arbitrary code on the affected system. The CVE website (http://cve.mitre.org/index.html) has numerous reported entries for fuzzing based vulnerabilities on 802.11 frames.

The system inspects each Probe Request frame looking for signs of fuzzing activity. Most common forms of Probe Request fuzzing involve expanding the SSID field beyond the limit of 32 bytes and changing the supported data rates to invalid rates. The system looks for these anomalies and will generate the Probe Request Fuzzing alarm when the field values are beyond the 802.11 specification.

Probe Response Fuzzed Frame Detected

Alarm Description and Possible Causes

802.11 Fuzzing is the process of introducing invalid, unexpected or random data into the 802.11 frames and then replaying those modified frames into the air. This can cause unexpected behavior to the destination device including driver crashes, operating system crashes and stack based overflows which would allow execution

of arbitrary code on the affected system. The CVE website (http://cve.mitre.org/index.html) has numerous reported entries for fuzzing based vulnerabilities on 802.11 frames.

The system inspects each Probe Response frame looking for signs of fuzzing activity. Most common forms of Probe Response fuzzing involve expanding the SSID field beyond the limit of 32 bytes and changing the supported data rates to invalid rates. The system looks for these anomalies and will generate the Probe Response Fuzzing alarm when the field values are beyond the 802.11 specification.

wIPS Solution

The system monitors the wireless network for traffic consistent with Probe Response Fuzzing. It is recommended to locate the device and take it offline.

Soft AP or Host AP Detected

Host AP tools: Cqure AP

Alarm Description and Possible Causes

A hotspot is any location where Wi-Fi network access available for the general public. Hotspots are often found in airports, hotels, coffee shops, and other places where business people tend to congregate. It is currently one of the most important network access service for business travelers. The customer requires a wireless-enabled laptop or handheld to connect to the legitimate access point and to receive service. Most hotspots do not require the user to have an advanced authentication mechanism to connect to the access point, other than using a web page to log in. The criterion for entry is only dependent on whether or not the subscriber has paid subscription fees. In a wireless hotspot environment, no one should trust anyone else. Due to current security concerns, some WLAN hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user.

Basic components of a WLAN Hotspot network

The four components of a basic hotspot network are as follows:

- Hotspot Subscribers—Valid users with a wireless enabled laptop or handheld and valid log in for accessing the hotspot network.

- WLAN Access Points—SOHO gateways or enterprise level access points depending upon the hotspot implementation.

- Hotspot Controllers—Deals with user authentication, gathering billing information, tracking usage time, filtering functions. This can be an independent machine or can be incorporated in the access point itself.

- Authentication Server—Contains the log in credentials for the subscribers. In most cases, hotspot controllers verify subscribers' credentials with the authentication server.

Hotspotter automates a method of penetration against wireless clients, independent of the encryption mechanism used. Using the Hotspotter tool, the intruder can passively monitor the wireless network for probe request frames to identify the SSIDs of the networks of the Windows XP clients.

After it acquires the preferred network information, the intruder compares the network name (SSID) to a supplied list of commonly used hotspot network names. When a match is found, the Hotspotter client acts as an access point. The clients then authenticate and associate unknowingly to this fake access point.

When the client gets associated, the Hotspotter tool can be configured to run a command such as a script to kick off a DHCP daemon and other scanning against the new victim.

Clients are also susceptible to this kind of attack when they are operating in different environments (home and office) while they are still configured to include the hotspot SSID in the Windows XP wireless connection settings. The clients send out probe requests using that SSID and make themselves vulnerable to the tool.

wIPS Solution

Soft APs or Software Access points should be treated as a Rogue device. The following steps should help eliminate this threat.

- Use integrated over-the-air physical location capabilities to locate the Rogue device

- Wireless Containment to prevent any devices from connecting to the Soft AP

- Trace the device on the wired network using rogue location discovery protocol (RLDP) or switch port tracing to find the rogue device

Spoofed MAC Address Detected

Alarm Description and Possible Causes

Spoofed mac address detected is a type of attack where a hacker will change their factory assigned wireless mac address to either gain access to a restricted wireless network by impersonating a valid connected user or to hide their presence on the wireless network.

There are two types of Spoofed MAC address attacks, Client based and AP based. For client based Spoofed MAC address attacks, the client could be trying to impersonate a valid user. An example of this would be a wireless hacker trying to get onto an access controlled hotspot by spoofing their wireless mac address of a client that is already connected, in effect "piggybacking" on the connection. Another popular example would be in a hotel environment where a hacker bypasses the payment process to get on the wireless network by spoofing their wireless mac address of a paid user.

Another type of Spoofed MAC address attack is AP based. In this case, the hacker is trying to hide their presence on the wireless network by spoofing the mac address of a corporate access point. This is a typical rogue scenario.

Suspicious After Hours Traffic Detected

Alarm Description and Possible Causes

One way to detect a wireless security penetration attempt is to match wireless usage against the time when there is not supposed to be any wireless traffic. The wIPS server monitors traffic patterns against the office-hours configured for this alarm to generate alerts when an abnormality is found. Specific suspicious wireless usage sought after by the wIPS server during after-office hours include the following:

- Client station initiating authentication or association requests to the office WLAN that may indicate security breach attempts.

• Wireless data traffic that may indicate suspicious download or upload over the wireless network.

wIPS Solution

For global wIPS deployment, the configurable office-hour range is defined in local time. The access point or sensor can be configured with a time zone to facilitate management. For the office and manufacturing floor mixed WLAN, one can define one set of office hours for the office WLAN SSID and another (for example, 6am to 9pm) for the manufacturing floor WLAN SSID. If this alarm is triggered, the administrator should look for devices responsible for the suspicious traffic and take appropriate steps to locate it and remove it from the wireless environment.

Unauthorized Association By Vendor List

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS enables network administrators to include vendor information in a policy profile to allow the system to effectively detect stations on the WLAN that are not made by approved vendors. Once such a policy profile is created, the system generates an alarm whenever an access point is associating with a station by an unapproved vendor. See the diagram below.

As the diagram shows, the access points in ACL-1 should only associate with stations made by Cisco and the access points in ACL-2 can only associate with stations manufactured by Intel. This information is entered in the wIPS system's policy profile. Any association between the access points and non-Cisco or non-Intel stations is unauthorized and triggers an alarm.

In the enterprise WLAN environment, rogue stations cause security concerns and undermine network performance. They take up air space and compete for network bandwidth. Since an access point can only accommodate a limited number of stations, it rejects association requests from stations once its capacity is reached. An access point laden with rogue stations denies legitimate stations the access to the network. Common problems caused by rogue stations include connectivity problems and degraded performance.

wIPS Solution

The Cisco Adaptive Wireless IPS automatically alerts network administrators to any unauthorized access point-station association involving non-conforming stations using this alarm. Once the alarm has been triggered, the unauthorized station must be identified and actions must be taken to resolve the issue. One way is to block it using the rogue containment.

Unauthorized Association Detected

Alarm Description and Possible Causes

In an enterprise network environment, rogue access points installed by employees do not usually follow the network's standard deployment practice and therefore compromise the integrity of the network. They are loopholes in network security and make it easy for intruders to hack into the enterprise wired network. One of the major concerns that most wireless network administrators face is unauthorized associations between

stations in an ACL and a rogue access point. Since data to and from the stations flows through the rogue access point, it leaves the door open for hackers to obtain sensitive information.

Rogue stations cause security concerns and undermine network performance. They take up air space and compete for bandwidths on the network. Since an access point can only serve a certain number of stations, it rejects association requests from stations once its capacity is reached. An access point laden with rogue stations denies legitimate stations access to the network. Common problems caused by rogue stations include disrupted connections and degraded performance.

wIPS Solution

The Cisco Adaptive Wireless IPS can automatically alert network administrators to any unauthorized access point-station association it has detected on the network through this alarm. The WLC new feature "MAC Address Learning" will prevent this violation from happening, it is recommended to enable this feature.

Wellenreiter Detected

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (i.e. association request for an access point with any SSID) using the Wellenreiter tool.

Wellenreiter is a commonly used tool for war-driving and war-chalking. A wireless hacker uses war-driving tools to discover access points and to publish their information (MAC address, SSID, security implemented, etc.) on the Internet with the access points' geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similar to war-driving, but the hacker is on foot instead of a car. War-walkers like to use Wellenreiter and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used, but from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.

The tool supports Prism2, Lucent, and Cisco based cards. The tool can discover infrastructure and ad-hoc networks that are broadcasting SSIDs, their WEP capabilities, and can provide vendor information automatically. It also creates an ethereal/tcpdump-compatible dumpfile and an Application savefile. It also has GPS support. Users can download the tool from Wellenreiter website.

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which of your access points is broadcasting an SSID in the beacons.

Cisco WCS also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, refer to the WCS online help.

WiFi Protected Setup Pin Brute Force

Alarm Description and Possible Causes

WiFi Protected Setup is a feature on most consumer grade Access Points that allows for easy device setup without the need for complex passwords. The feature allows the user to either use the push button method or enter in the pin found on the bottom of the Access Point to connect. A vulnerability was announced in December 2011 by Stefan Viehböck and independently discovered by Craig Heffner. The vulnerability is with the external registrar that only requires the devices pin. This mode is susceptible to brute force attacks against the pin. There are currently 2 active tools in the wild exploiting this.

The basic idea behind the attack is when a pin authentication fails, the access point sends back an EAP-NACK message to the client. With this EAP-NACK message, the attacker is able to determine if the first half of the pin is correct. The last digit of the pin is known since it is a checksum for the pin. This reduces the attempts to brute force the pin down to 11,000.

It is recommended to disable the external registrar feature of WiFi Protected Setup on your Access Point. Most manufacturers have this feature on by default.

wIPS Solution

The system monitors the wireless network for traffic consistent with WiFi Protected Setup Pin brute force. It is recommended to locate the device and take it offline.

WiFi Tap Tool Detected

Alarm Description and Possible Causes

The WiFiTap tool allows a wireless attacker to configure a client to communicate directly with another client, without connecting to a corporate AP. This implementation allows the intruder to target an attack against the individual client, bypassing any security measures configured on the corporate network. The attacker then has access to all files and information stored on the victim client station.

wIPS Solution

The wIPS server monitors for use of the WiFiTap tool and triggers an alarm if it is detected. Users should attempt to locate the attacking device and remove it from the wireless environment.

Performance Violation

WLAN performance efficiency is constantly challenged by the dynamics of the RF environment and the mobility of client devices. A closely monitored and well tuned WLAN system can achieve a higher throughput than a poorly managed one. Cisco wIPS ensures WLAN performance and efficiency by monitoring the WLAN on a continued basis and alerting the wireless administrator on early warning signs for trouble.

To maximize the power of Cisco wIPS, performance alarms can be customized to best match your WLAN deployment specification.

Performance Violation include the following subcategory:

Channel or Device Overload

WLAN technologies use the radio frequency spectrum as a shared physical media similar to the original 10 Mbps Ethernet technology. Even for the latest WLAN standards for 802.11a and 802.11g, there is still a 54 Mbps shared media bandwidth ceiling. In reality, the ceiling is much lower considering the necessary MAC protocol overhead, inter-frame spacing, collision, and random transmission back-offs.

The radio medium has its own bandwidth limitations. WLAN Access Points have limitations that can be overloaded by heavy traffic or a large number of associated clients. Like the wired LAN, excessive multicast and broadcast frames can put extra burden on the WLAN devices. Overloaded devices suffer from degraded performance and cause connectivity problems. For example, AP association table overflowed by large number of clients.

Be it channel bandwidth limitation or the WLAN device resource capacity, Cisco wIPS, monitors and tracks the load to ensure smooth operation. Cisco wIPS raises alarms and offers specific details in scenarios where WLAN's performance is not satisfactory due to under-provisioning or over-growth. RF has no boundaries that lead to your WLAN channel utilization, to increase significantly even when your neighbor installs new WLAN devices in an adjoining channel. Cisco wIPS monitors your WLAN to ensure proper bandwidth and resource provisioning.

Performance Violation include the following types:

AP Association Capacity Full

Alarm Description and Possible Causes

All WLAN Access Points have a resource limit for the number of client stations that can associate to it ,to receive wireless services. Usually, this limit is a user configurable number on the AP. After an AP reaches this limit, it will not accept any more new client association requests.

wIPS Solution

Cisco wIPS monitors on rejected association requests and responses to determine the cause of failed associations. This alarm is generated when Cisco wIPS concludes that it is caused due to AP association capacity overflow problem. This alarm indicates under-provisioning or failed load balancing for the WLAN deployment.

AP Overloaded by Stations

Alarm Description and Possible Causes

A WLAN Access Point can service only a limited number of clients due to limited resources . When the limit is reached, additional clients are rejected in service, or degraded performance for the existing clients. When designing a WLAN equipment deployment and provisioning for service, this limitation should be considered.

After deployment, the limitation may be challenged by the growing number of users and thereby requires constant monitoring for under-provisioned deployment.

wIPS Solution

Cisco wIPS monitors the AP work load by tracking its active client stations. You can configure the system to generate alarms of different severity levels by the work load threshold (active client session count).For example, warning alarm for 64 active client sessions and urgent alarms for 128 active client sessions.

AP Overloaded by Utilization

Alarm Description and Possible Causes

A WLAN design for deployment includes an expectation for the maximum clients an AP can support. Similarly, there is an expectation for the maximum bandwidth utilization supported by an AP. Such expectations can be used to monitor on sufficient WLAN provisioning and effective load-balancing.

wIPS Solution

Cisco wIPS tracks AP bandwidth utilization (the sum of outgoing and incoming traffic combined) and raises an alarm when the sustained utilization exceeds the user configured threshold.

Excessive Bandwidth Usage

Alarm Description and Possible Causes

The WLAN spectrum is a shared medium with a limitation on bandwidth. Be it 802.11b at 11 mbps or 802.11a/g at 54 mbps, bandwidth utilization should be closely monitored on a per channel and per device basis to ensure sufficient WLAN provisioning for all client devices. Please note that high bandwidth consumption does not mean high WLAN throughput. The problem lies in the low speed transmission, and could also be due to an authorized user who is downloading music or movies from the Internet causing the bandwidth of the corporate network to choke. Cisco wIPS tracks WLAN bandwidth utilization on a per channel and per device basis

wIPS Solution

Cisco wIPS tracks bandwidth utilization based on channel and wireless device. The bandwidth calculation includes the PLCP header, preamble, and the actual frame payload. Because of the CSMA collision avoidance protocol, it is practically impossible to get even close to 100% utilization. 60 to 70% of utilization should be considered extremely high and requires better provisioning or improved efficiency such as strict high speed transmission. When the user defined threshold (in percentage of utilization) is exceeded, Cisco wIPS raises this alarm. Take appropriate steps to tackle this problem. This could include finding users who may be causing this due to excessive file downloading from the Internet.

Excessive Multicast/Broadcast on Channel

Alarm Description and Possible Causes

Like the wired network, excessive broadcast and multicast frames on the WLAN impose an extra load on all devices on the WLAN. WLAN is more sensitive to multicast and broadcast frames than the wired networks because all multicast and broadcast frames are transmitted at low speed (for example, 1 or 2 mbps for 802.11b WLAN). Such low speed transmissions consume more WLAN bandwidth. Besides bandwidth inefficiency, low speed multicast and broadcast frames take longer to complete the transmission process thus introducing higher delays for other devices waiting for the wireless medium to be free. Excessive multicast and broadcast frames introduce jitters to delay-sensitive WLAN applications such as **VoIP**. For example, a 1000-byte broadcast frame would take at least 8 milliseconds to transmit at 1 mpbs, which is a considerable delay for a voice application.

wIPS Solution

Cisco wIPS tracks multicast and broadcast frame usage on a per channel and per device basis to report abuse. The alarm threshold is the percentage of multicast and broadcast frames to total frames by the device or channel.

Excessive Multicast/Broadcast on Node

Alarm Description and Possible Causes

Just like the wired network, excessive broadcast and multicast frames on the WLAN impose an extra load on all devices on the WLAN. WLAN is sensitive to multicast and broadcast frames than the wired networks because of the low speed at which all the multicast and broadcast frames are transmitted (for example, 1 or 2 mbps for 802.11b WLAN). Such low speed transmissions consume more WLAN bandwidth. Besides bandwidth inefficiency, low speed multicast and broadcast frames take longer to complete the transmission process thus introducing higher delays for other devices waiting for the wireless medium to be free. Excessive multicast and broadcast frames introduce jitters to delay-sensitive WLAN applications such as **VoIP**. For example, a 1000-byte broadcast frame would take at least 8 milliseconds to transmit at 1 mpbs, which is a considerable delay for a voice application.

wIPS Solution

Cisco wIPS tracks multicast and broadcast frame usage on a per channel and per device basis to report abuse. The alarm threshold is the percentage of multicast and broadcast frames to total frames by the device or channel.

APPENDIX **B**

Rogue Management

This appendix describes security issues and solutions for rogue access points.

This appendix contains the followings sections:

Rogue Access Point Challenges

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

The operating system security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access points, automatically discover rogue access points, and locate them as described in the Rogue Access Point Location, Tagging, and Containment, on page 223 section.

Rogue Access Point Location, Tagging, and Containment

When the Cisco Unified Wireless Network Solution is monitored using the Prime Infrastructure, the Prime Infrastructure generates the flags as rogue access point traps and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the access points closest to each rogue access point. The next step is to mark them as Known or Acknowledged rogue access points (no further action), Alert rogue access points (watch for and notify when active), or Contained rogue access points (have

between one and four access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

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

- Locate rogue access points

- Receive new rogue access point notifications, eliminating hallway scans

- Monitor unknown rogue access points until they are eliminated or acknowledged

- Determine the closest authorized access point, making directed scans faster and more effective

- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment can be done for individual rogue access points by MAC address or can be mandated for all rogue access points connected to the enterprise subnet.

- Tag rogue access points:

  ◦ Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or wireless LAN security

  ◦ Accept rogue access points when they do not compromise the LAN or wireless LAN security

  ◦ Tag rogue access points as unknown until they are eliminated or acknowledged

  ◦ Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

Detecting and Locating Rogue Access Points

When the access points on your wireless LAN are powered up and associated with controllers, the Prime Infrastructure immediately starts listening for rogue access points. When a controller detects a rogue access point, it immediately notifies the Prime Infrastructure, which creates a rogue access point alarm.

When the Prime Infrastructure receives a rogue access point message from a controller, an alarm monitor appears in the lower left corner of all the Prime Infrastructure user interface page.

To detect and locate rogue access points, follow these steps:

Step 1 Click the Rogues indicator to display the Rogue AP Alarms page. This page lists the severity of the alarms, the rogue access point MAC addresses, the rogue access point types, the date and time when the rogue access points were first detected, and their SSIDs.

Step 2 Click any Rogue MAC Address link to display the associated Alarms > Rogue - AP MAC Address page. This page shows detailed information about the rogue access point alarm.

Step 3 To modify the alarm, choose one of these commands from the Select a command drop-down list, and click **Go**.

- Assign to me—Assigns the selected alarm to the current user.

- Unassign—Unassigns the selected alarm.

- Delete—Deletes the selected alarm.

- Clear—Clears the selected alarm.

- Event History—Enables you to view events for rogue alarms.

- Detecting APs (with radio band, location, SSID, channel number, WEP state, short or long preamble, RSSI, and SNR)—Enables you to view the access points that are currently detecting the rogue access point.

- Rogue Clients—Enables you to view the clients associated with this rogue access point.

- Set State to `Unknown - Alert'—Tags the rogue access point as the lowest threat, continues to monitor the rogue access point, and turns off containment.

- Set State to `Known - Internal'—Tags the rogue access point as internal, adds it to the known rogue access points list, and turns off containment.

- 1 AP Containment through 4 AP Containment—When you select level 1 containment, one access point in the vicinity of the rogue unit sends deauthenticate and disassociate messages to the client devices that are associated to the rogue unit. When you select level 2 containment, two access points in the vicinity of the rogue unit send deauthenticate and disassociate messages to the rogue's clients and so on up to level 4.

Step 4   From the Select a command drop-down list, choose **Map (High Resolution),** and click **Go** to display the current calculated rogue access point location in the Maps > Building Name > Floor Name page.
If you are using the Prime Infrastructure Location, the Prime Infrastructure compares RSSI signal strength from two or more access points to find the most probable location of the rogue access point and places a small skull-and-crossbones indicator at its most likely location. In the case of an underdeployed network for location with only one access point and an omni antenna, the most likely location is somewhere on a ring around the access point, but the center of likelihood is at the access point. If you are using the Prime Infrastructure Base, Prime Infrastructure relies on RSSI signal strength from the rogue access point and places a small skull-and-crossbones indicator next to the access point receiving the strongest RSSI signal from the rogue unit.

Monitoring Alarms

This section contains the following topics:

Monitoring Rogue Access Point Alarms

Rogue access point radios are unauthorized access points detected by one or more Cisco lightweight access points. This page displays rogue access point alarms based on the severity you clicked in the Alarm Monitor.

To access the Rogue AP Alarms page, do one of the following:

• Choose **Monitor** > **Alarms**. Click **Search** and choose **Rogue AP** from the Alarm Category drop-down list. Click **Go** to display the matching alarms.

• Choose **Monitor** > **Security**. From the left sidebar, choose **Rogue AP**.

• Click the **Malicious AP** number link in the Alarm Summary box of the left sidebar menu.

Note   If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use the scroll arrows to view additional alarms.

The below table describes the parameters found in the Rogue Access Point Alarms page

Table 26: Alarm Parameters

Parameter	Description
Check box	Select the alarms on which you want to take action.
Severity	The severity of the alarm: Critical, Major, Minor, Clear, Color coded.
Rogue Adhoc MAC Address	Media Access Control address of the rogue ad hoc.
Vendor	Rogue ad hoc vendor name, or Unknown.
Classification Type	Malicious, Friendly, or Unclassified.
Radio Type	Indicates the radio type for this rogue ad hoc.
Strongest AP RSSI	Indicates the strongest Received Signal Strength Indicator in dBm.
No. of Rogue Clients	Indicates the number of rogue clients associated to this rogue ad hoc.
Owner	Indicates the 'owner' of the rogue ad hoc.
Date/Time	Date and time the alarm occurred.
State	State of the alarm: Alert, Known or Removed.
SSID	Service Set Identifier being broadcast by the rogue ad hoc radio. (Blank if the SSID is not broadcast.)
Map Location	Indicates the map location for this rogue ad hoc.

Acknowledged	Displays whether or not the alarm is acknowledged by the user.

You can select one or more alarms by selecting their respective check boxes, choosing one of the following commands from the Select a command drop-down list, and click **Go**.

- **Assign to me**—Assigns the selected alarm(s) to the current user.

- **Unassign**—Unassigns the selected alarm(s).

- **Delete**—Deletes the selected alarm(s).

- **Clear**—Clears the selected alarm(s).

- **Acknowledge**—Acknowledges the alarm to prevent it from showing up in the Alarm Summary page.

> **Note** The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.

- **Unacknowledge**—Unacknowledges an already acknowledged alarm.

- Email Notification—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications.

- **Detecting APs**—View the Cisco Aironet 1000 Series lightweight access points that are currently detecting the rogue ad hoc. See Detecting Access Points on a Network for more information.

- **Map (High Resolution)**—Click to display a high-resolution map of the rogue ad hoc location.

- **Rogue Clients**—Click to view a list of rogue clients associated with this rogue ad hoc. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the rogue ad hoc.

- **Set State to 'Alert'**—Choose this command to tag the rogue ad hoc as the lowest threat, continue monitoring the rogue access point, and to turn off Containment.

- **Set State to 'Internal'**—Choose this command to tag the rogue ad hoc as internal, add it to the Known Rogue APs list, and to turn off Containment.

- **Set State to 'External'**—Choose this command to tag the rogue ad hoc as external, add it to the Known Rogue APs list, and to turn off Containment.

- **1 AP Containment**—Targets the rogue ad hoc for containment by one access point. (Lowest containment level.)

- **2 AP Containment**—Targets the rogue ad hoc for containment by two Cisco Aironet 1000 Series lightweight access points.

- **3 AP Containment**—Targets the rogue ad hoc for containment by three Cisco Aironet 1000 Series lightweight access points.

- **4 AP Containment**—Targets the rogue ad hoc for containment by four Cisco Aironet 1000 Series lightweight access points. (Highest containment level.)

⚠

Caution   Attempting to contain a rogue AP may lead to legal consequences. When you select any of the AP Containment commands and click **Go**, a message "Containing a Rogue AP may have legal consequences. Do you want to continue?" appears. Click **OK** if you are sure, or click **Cancel** if you do not want to contain any access points.

Monitoring Rogue AP Details

Alarm event details for each rogue access point are available in the Rogue AP Alarms page. To view alarm events for a rogue access point radio, in the Rogue AP Alarms page, click an item under Rogue MAC Address.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by Cisco lightweight access points. The following information is available:

- General Info:

  - Rogue MAC Address—Media Access Control address of the rogue access points.

  - Vendor—Rogue access point vendor name or Unknown.

  - On Network—Indicates whether or not the rogue access point is located on the network.

  - Owner—Indicates the owner or left blank.

  - Acknowledged—Indicates whether or not the alarm is acknowledged by the user.

  - Classification Type—Malicious, Friendly, or Unclassified.

  - State—Indicates the state of the alarm: Alert, Known, or Removed.

  - SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

  - Channel Number—Indicates the channel of the rogue access point.

  - Containment Level—Indicates the containment level of the rogue access point or Unassigned.

  - Radio Type—Indicates the radio type for this rogue access point.

  - Strongest AP RSSI—Indicates the strongest received signal strength indicator in dBm.

  - No. of Rogue Clients—Indicates the number of rogue clients associated to this access point.

  - Created—Indicates when the alarm event was created.

  - Modified—Indicates when the alarm event was modified.

  - Generated By—Indicates how the alarm event was generated.

  - Severity—The severity of the alarm: Critical, Major, Minor, Clear, Color coded.

  - Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear, Color coded.

- Annotations—Enter any new notes in this text box and click Add to update the alarm.

- Message—Displays descriptive information about the alarm.

• Help—Displays the latest information about the alarm.

• Event History—Click to access the Monitor Alarms > Events page.

• Annotations—Lists existing notes for this alarm.

Detecting Access Points

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

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

• Perform a search for rogue APs.

• From the NCS home page, click the Security dashboard. This dashboard displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.

• Click the **Malicious AP** number link in the Alarm Summary box.

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

Step 3   From the Select a command drop-down list, choose **Detecting APs**.

Step 4   Click **Go.**
Click a list item to display data about that item:

• AP Name

• Radio

• Map Location

• SSID—Service Set Identifier being broadcast by the rogue access point radio.

• Channel Number—Which channel the rogue access point is broadcasting on.

• WEP—Enabled or disabled.

• WPA—Enabled or disabled.

• Pre-Amble—Long or short.

• RSSI—Received signal strength indicator in dBm.

• SNR—Signal-to-noise ratio.

• Containment Type—Type of containment applied from this access point.

• Containment Channels—Channels that this access point is currently containing.

Monitoring Rogue Ad hoc Alarms

The rogue Ad hoc Alarms page displays alarm events for rogue ad hocs.

To access the Rogue Adhoc Alarms page, do one of the following:

- Choose **Monitor** > **Alarms**. From the lest sidebar menu, click **Search** and choose **Adhoc** from the Alarm Category drop-down list. Click **Go** to display the matching alarms.

- Choose **Monitor** > **Alarms**. From the left sidebar, choose **New Search**, and choose **Rogue Adhoc** from the Alarm Category drop-down list. Click **Go** to display the matching alarms.

- Click the **Monitor** > **Security**. From the left sidebar menu, choose Rogue Adhocs.

Note If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use the scroll arrows to view additional alarms.

The below table describes the parameters found in the Rogue Ad hoc Alarms page.

Table 27: Alarm Parameters

Parameter	Description
Check box	Select the alarms on which you want to take action.
Severity	The severity of the alarm: Critical, Major, Minor, Clear, Color coded.
Rogue Adhoc MAC Address	Media Access Control address of the rogue ad hoc.
Vendor	Rogue ad hoc vendor name, or Unknown.
Classification Type	Malicious, Friendly, or Unclassified.
Radio Type	Indicates the radio type for this rogue ad hoc.
Strongest AP RSSI	Indicates the strongest Received Signal Strength Indicator in dBm.
No. of Rogue Clients	Indicates the number of rogue clients associated to this rogue ad hoc.
Owner	Indicates the 'owner' of the rogue ad hoc.
Date/Time	Date and time the alarm occurred.
State	State of the alarm: Alert, Known or Removed.
SSID	Service Set Identifier being broadcast by the rogue ad hoc radio. (Blank if the SSID is not broadcast.)
Map Location	Indicates the map location for this rogue ad hoc.

Acknowledged	Displays whether or not the alarm is acknowledged by the user.

You can select one or more alarms by selecting their respective check boxes, choosing one of the following commands from the Select a command drop-down list, and click **Go**.

- **Assign to me**—Assigns the selected alarm(s) to the current user.

- **Unassign**—Unassigns the selected alarm(s).

- **Delete**—Deletes the selected alarm(s).

- **Clear**—Clears the selected alarm(s).

- **Acknowledge**—Acknowledges the alarm to prevent it from showing up in the Alarm Summary page.

> **Note** The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.

- **Unacknowledge**—Unacknowledges an already acknowledged alarm.

- **Email Notification**—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications.

- **Detecting APs**—View the Cisco Aironet 1000 Series lightweight access points that are currently detecting the rogue ad hoc. See Detecting Access Points on a Network for more information.

- **Map (High Resolution)**—Click to display a high-resolution map of the rogue ad hoc location.

- **Rogue Clients**—Click to view a list of rogue clients associated with this rogue ad hoc. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the rogue ad hoc.

- **Set State to 'Alert'**—Choose this command to tag the rogue ad hoc as the lowest threat, continue monitoring the rogue access point, and to turn off Containment.

- **Set State to 'Internal'**—Choose this command to tag the rogue ad hoc as internal, add it to the Known Rogue APs list, and to turn off Containment.

- **Set State to 'External'**—Choose this command to tag the rogue ad hoc as external, add it to the Known Rogue APs list, and to turn off Containment.

- **1 AP Containment**—Targets the rogue ad hoc for containment by one access point. (Lowest containment level.)

- **2 AP Containment**—Targets the rogue ad hoc for containment by two Cisco Aironet 1000 Series lightweight access points.

- **3 AP Containment**—Targets the rogue ad hoc for containment by three Cisco Aironet 1000 Series lightweight access points.

- **4 AP Containment**—Targets the rogue ad hoc for containment by four Cisco Aironet 1000 Series lightweight access points. (Highest containment level.)

⚠️

Caution Attempting to contain a rogue AP may lead to legal consequences. When you select any of the AP Containment commands and click **Go**, a message "Containing a Rogue AP may have legal consequences. Do you want to continue?" appears. Click **OK** if you are sure, or click **Cancel** if you do not want to contain any access points.

Monitoring Rogue Ad hoc Details

Alarm event details for each rogue ad hoc are available in the Rogue Adhoc Alarms page.

To view alarm events for a rogue ad hoc radio, in the Rogue Adhoc Alarms page, click an item under Rogue MAC Address.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by Cisco Aironet 1000 Series lightweight access points. The following information is available:

- General:

    ◦ Rogue MAC Address—Media Access Control address of the rogue ad hoc.

    ◦ Vendor—Rogue ad hoc vendor name or Unknown.

    ◦ On Network—Indicates whether or not the rogue ad hoc is located on the network.

    ◦ Owner—Indicates the owner or left blank.

    ◦ Acknowledged—Indicates whether or not the alarm is acknowledged by the user.

    ◦ Classification Type—Malicious, Friendly, or Unclassified.

    ◦ State—Indicates the state of the alarm: Alert, Known, or Removed.

    ◦ SSID—Service Set Identifier being broadcast by the rogue ad hoc radio. (Blank if the SSID is not broadcast.)

    ◦ Channel Number—Indicates the channel of the rogue ad hoc.

    ◦ Containment Level—Indicates the containment level of the rogue ad hoc or Unassigned.

    ◦ Radio Type—Indicates the radio type for this rogue ad hoc.

    ◦ Strongest AP RSSI—Indicates the strongest Received Signal Strength Indicator in dBm.

    ◦ No. of Rogue Clients—Indicates the number of rogue clients associated to this ad hoc.

    ◦ Created—Indicates when the alarm event was created.

    ◦ Modified—Indicates when the alarm event was modified.

    ◦ Generated By—Indicates how the alarm event was generated.

    ◦ Severity—The severity of the alarm: Critical, Major, Minor, Clear, and Color coded.

    ◦ Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear, and Color coded.

- Annotations—Enter any new notes in this text box, and click Add to update the alarm.

- Message—Displays descriptive information about the alarm.

- Help—Displays the latest information about the alarm.

- Annotations—Lists existing notes for this alarm.

Select a Command

Select one or more alarms by selecting their respective check boxes, choosing one of the following commands, and clicking **Go**.

- Assign to me—Assigns the selected alarm to the current user.

- Unassign—Unassigns the selected alarm.

- Delete—Deletes the selected alarm.

- Clear—Clears the selected alarm.

- Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—You can choose to unacknowledge an already acknowledged alarm.

- Email Notification—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications.

- Detecting APs—View the Cisco Aironet 1000 Series lightweight access points that are currently detecting the rogue ad hoc.

- Map (High Resolution)—Click to display a high-resolution map of the rogue ad hoc location.

- Rogue Clients—Click to view a list of rogue clients associated with this rogue ad hoc. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the rogue ad hoc.

- Set State to 'Alert'—Choose this command to tag the rogue ad hoc as the lowest threat, continue monitoring the rogue ad hoc, and to turn off Containment.

- Set State to 'Internal'—Choose this command to tag the rogue ad hoc as internal, add it to the Known Rogue APs list, and to turn off Containment.

- Set State to 'External'—Choose this command to tag the rogue access point as external, add it to the Known Rogue APs list, and to turn off Containment.

- 1 AP Containment—Targets the rogue ad hoc for containment by one access point. (Lowest containment level.)

- 2 AP Containment—Targets the rogue ad hoc for containment by two Cisco Aironet 1000 Series lightweight access points.

- 3 AP Containment—Targets the rogue ad hoc for containment by three Cisco Aironet 1000 Series lightweight access points.

- 4 AP Containment—Targets the rogue ad hoc for containment by four Cisco Aironet 1000 Series lightweight access points. (Highest containment level.)

Monitoring Events

Click a Rogues alarm square in the Alarm Monitor, click a list item under Rogue MAC Addresses, from the Select a command drop-down list, choose Event History, and click Go to access this page.

Choose Monitor > Alarms and then choose New Search from the left sidebar menu. Choose Severity > All Severities and Alarm Category > Rogue AP, and click Go to access the Monitor Alarms > failure object page. Click an item under the Rogue MAC Address to display the Monitor Alarms > Rogue AP Details page. From the Select a command drop-down list, choose Event History, and click Go to access this page.

This page enables you to review information about rogue alarm events. Events list the sequence of occurrences for an element(s) over a period of time.

Click the title of each column to reorder the listings:

- Severity—Color-coded display of the severity of the event.

- Rogue MAC Address—Click a list item to display information about the entry.

- Vendor—Name of rogue access point manufacturer.

- Type—AP or AD-HOC.

- On Network—Whether or not the rogue access point is on the same subnet as the associated port.

- On 802.11b—Whether or not the rogue access point is broadcasting on the 802.11b/802.11g band.

- Date/Time—Date and time of the alarm.

- Classification Type—Malicious, Friendly, or Unclassified.

- State—State of the alarm, such as Alert and Removed.

- SSID—Service Set Identifier being broadcast by the rogue access point radio.

- On 802.11a—Whether or not the rogue access point is broadcasting on the 802.11a band.

Monitoring Rogue Clients

Choose **Monitor** > **Alarms** and then choose New Search from the left sidebar menu. Choose **Severity** > **All Severities** and **Alarm Category** > **Rogue AP**, and click **Go** to access the Monitor Alarms > failure object page. Click an item under the Rogue MAC Address to display the Monitor Alarms > Rogue AP Details page. From the Select a command drop-down list, choose **Rogue Clients** to access this page.

This page enables you to view the following information about clients that have associated with the rogue access point:

- Client MAC Address—Media Access Control address of the rogue access point client.

- Last Heard—The last time a Cisco access point detected the rogue access point client.

- Status—Status of the rogue access point client.

Configuring Auto SPT Criteria on Prime Infrastructure

To configure auto switch port tracing settings on the Prime Infrastructure, follow these steps:

Step 1   Choose **Administration** > **System Settings**.

Step 2   From the left sidebar menu, choose **Rogue AP Settings**.
The Rogue AP Settings page appears.

Step 3   Select the **Enable Auto Switch Port Tracing** check box to allow the Prime Infrastructure to automatically trace the switch port to which the rogue AP is connected. You can configure the following parameters:

- Repeat Search After—Enter the number of minutes after which you want the Prime Infrastructure to automatically repeat the search for rogue APs. By default, the Prime Infrastructure repeats the search for rogue APs every 120 minutes.

- Allow Trace For Found On Wire Rogue AP—Select the check box to enable auto SPT to trace wired rogue APs.

- Critical—Select the check box to set the alarm severity to critical.

- Major—Select the check box to set the alarm severity to major.

- Minor—Select the check box to set the alarm severity to minor.

Step 4   Click **OK**.

Configuring Auto Containment Settings on the Prime Infrastructure

To configure auto containment settings on the Prime Infrastructure, follow these steps:

Step 1   Choose **Administration** > **Settings**.

Step 2   From the left sidebar menu, choose **Rogue AP Settings**.
The Rogue AP Settings page appears.

Step 3   Select the **Enable Auto Containment** check box to allow the Prime Infrastructure to trigger auto containment when a rogue AP is received by the Prime Infrastructure. You can configure the following auto containment parameters:

- Exclude Rogue APs Found On Wire By Switch Port Tracing—Select the check box to automatically exclude those rogue APs that are detected on the wired network through auto SPT.

- Critical—Select the check box to set the alarm severity to critical.

- Major—Select the check box to set the alarm severity to major.

- Containment Level—Select the check box to enable the auto containment level. This indicates the containment level of the rogue APs.

◦ 1 AP Containment through 4 AP Containment—Set the auto containment level by entering a value between 1 and 4. When you select level 1 containment, one access point in the vicinity of the rogue unit sends deauthenticate and disassociate messages to the client devices that are associated with the rogue unit. When you select level 2 containment, two access points in the vicinity of the rogue unit send deauthenticate and disassociate messages to the client devices and so on up to level 4.

Note   The higher the threat of the rogue access point, the higher the containment required.

Caution   Attempting to contain a rogue access point might lead to legal consequences. When you select any of the AP Containment commands and click Go, a message "Containing a Rogue AP may have legal consequences. Do you want to continue?" appears. Click OK if you are sure or click Cancel if you do not want to contain any access points.

Step 4   Click **OK**.

Configuring Controllers

This section contains the following topics:

- Configuring Rogue Policies, on page 236
- Configuring Rogue AP Rules, on page 237

Configuring Rogue Policies

This page enables you to set up policies for rogue access points.

To access the Rogue Policies page, follow these steps:

Step 1   Choose **Configure > Controllers.**

Step 2   Click an IP address in the IP Address column.

Step 3   From the left sidebar menu, choose **Security > Rogue Policies**

- Rogue Location Discovery Protocol—Enabled, Disabled.
- Rogue APs

  ◦ Expiration Timeout for Rogue AP Entries (seconds)—1 - 3600 seconds (1200 default).

- Rogue Clients

  ◦ Validate rogue clients against AAA (check box)—Enabled, Disabled.

  ◦ Detect and report ad hoc networks (check box)—Enabled, Disabled command buttons.

- Save—Saves the changes made to the client exclusion policies and returns to the previous page.

• Audit—Compares the NCS values with those used on the controller.

Configuring Rogue AP Rules

This page enables you to view and edit current rogue AP rules.

To access the Rogue AP Rules page, follow these steps:

Step 1   Choose **Configure >** Controllers.

Step 2   Click an IP address in the IP Address column.

Step 3   From the left sidebar menu, choose **Security > Rogue AP Rules**. The Rogue AP Rules page displays the rogue AP rules, the rule types (Malicious or Friendly), and the rule sequence.

Step 4   Select a rogue AP rule to view or edit its details.

Configuring Controller Template

This section contains the following topics:

Configuring Rogue Policies

To view current templates and the number of controllers to which they are applied, choose **Configure > Controller Templates > Security > Rogue Policies**

To create a new rogue policy template, follow these steps:

Step 1   Choose **Configure > Controller Templates**.

Step 2   From the left sidebar menu, choose **Security > Rogue Policies**.

Step 3   From the Select a command drop-down list, choose **Add Template**.

Step 4   Click **Go**.

    Note   To make modifications to an existing rogue policy template or to apply a current template to controllers, choose **Configure > Controller Templates > Security > Rogue Policies**, and click a template name in the Template Name column. Make the necessary changes to the template and click **Save** or **Apply to Controllers**.

Step 5 Select the **Rogue Location Discovery Protocol** check box to enable it. Rogue Location Discovery Protocol (RLDP) determines whether or not the rogue is connected to the enterprise wired network.

> **Note** With RLDP, the controller instructs a managed access point to associate with the rogue access point and send a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points that do not have encryption enabled.

Step 6 Set the expiration timeout (in seconds) for rogue access point entries.

Step 7 Select the **Validate rogue clients against AAA** check box to enable the AAA validation of rogue clients.

Step 8 Select the **Detect and report Adhoc networks** check box to enable detection and reporting of rogue clients participating in ad hoc networking

Step 9 Click any of these buttons:

- Save—Click to save the current template.

- **Apply to Controllers**—Click to apply the current template to controllers. In the Apply to Controllers page, select the applicable controllers, and click **OK**.

- **Delete**—Click to delete the current template. If the template is currently applied to controllers, click **OK** to confirm that you want to remove the template from the selected controllers to which it is applied.

- **Cancel**—Click to cancel the current template creation or changes to the current template.

Configuring Rogue AP Rules

Rogue AP rules allow you to define rules to automatically classify rogue access points. The NCS applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue on maps, based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

> **Note** Rogue AP rules also help reduce false alarms.
>
> To view current classification rule templates, rule type, and the number of controllers to which they are applied, choose **Configure > Controller Templates > Security > Rogue AP Rules**.

Note   Rogue classes include the following types: Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category. Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules. Unclassified Rogue—A detected access point that does not match the Malicious or Friendly rules.

To create a new classification rule template for rogue access points, follow these steps:

Step 1   Choose **Configure > Controller Templates**.

Step 2   From the left sidebar menu, choose **Security > Rogue AP Rules**.

Step 3   From the Select a command drop-down list, choose **Add Classification Rule**.

Step 4   Click **Go**.

Note   To make modifications to an existing Rogue AP Rules template or to apply a current template to controllers, choose **Configure > Controller Templates > Security > Rogue AP Rules** and click a template name in the Template Name column. Make the necessary changes to the template and click **Save** or **Apply to Controllers**.

Step 5   Complete the following fields:

- General:

    ◦ Rule Name—Enter a name for the rule in the text box.

    ◦ Rule Type—Choose **Malicious** or **Friendly** from the drop-down list.

    Note   Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category. Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.

    ◦ Match Type—Choose **Match All Conditions** or **Match Any Condition** from the drop-down list.

- Malicious Rogue Classification Rule

    ◦ Open Authentication—Select the check box to enable Open Authentication.

    ◦ Match Managed AP SSID—Select the check box to enable thematching of managed AP SSID rule condition.

    Note   Managed SSID are the SSIDs configured for the WLAN and is known to the system.

    ◦ Match User Configured SSID—Select the check box to enable the matching of user configured SSID rule condition.

    Note   User Configured SSID are the SSIDs that are manually added. Enter the User Configured SSIDs (one per line) in the Match User Configured SSID text box.

    ◦ Minimum RSSI—Select the check box to enable the Minimum RSSI threshold limit.

    Note   Enter the minimum RSSI threshold level (dB) in the text box. The detected access point is classified as malicious if it is detected above the indicated RSSI threshold.

    ◦ Time Duration—Select the check box to enable the Time Duration limit.

    Note   Enter the time duration limit (in seconds) in the text box. The detected access point is classified as malicious if it is viewed for a longer period of time than the indicated time limit.

◦ Minimum Number Rogue Clients—Select the check box to enable the Minimum Number Rogue Clients limit.

Note   Enter the minimum number of rogue clients allowed. The detected access point is classified as malicious if the number of clients associated to the detected access point is greater than or equal to the indicated value.

Step 6   Click any of the following buttons:

- **Save**—Click to save the current template.

- **Apply to Controllers**—Click to apply the current template to controllers. In the Apply to Controllers page, select the applicable controllers and click **OK**.

- **Delete**—Click to delete the current template. If the template is currently applied to controllers, click **OK** to confirm that you want to remove the template from the selected controllers to which it is applied.

- **Cancel**—Click to cancel the current template creation or changes to the current template.

Configuring Rogue AP Rule Groups

The Rogue AP Rule Group template allows you to combine more than one rogue AP rule to apply to controllers.

To view current Rogue AP Rule Group templates, choose **Configure > Controller Templates > Security > Rogue AP Rule Groups**.

To configure rogue AP rule groups, follow these steps:

Step 1   Choose **Configure > Controller Templates**.

Step 2   From the left sidebar menu, choose **Security > Rogue AP Rule Groups**.

Step 3   From the Select a command drop-down list, choose **Add Rogue Rule Group**.

Step 4   Click **Go**.

Note   To make modifications to an existing rogue policy template or to apply a current template to controllers, choose **Configure > Controller Templates > Security > Rogue AP Rule Groups** and click a template name in the Template Name column. Make the necessary changes to the template and click **Save** or **Apply to Controllers**.

Step 5   Enter the following parameters:

- General

◦ Rule Group Name—Enter a name for the rule group in the text box.

Step 6   To add a Rogue AP rule, click to highlight the rule in the left column. Click **Add** to move the rule to the right column.

Note   Rogue AP rules can be added from the Rogue AP Rules group box. See Configuring Rogue AP Rules for more information.

Step 7   To remove a Rogue AP rule, click to highlight the rule in the right column. Click **Remove** to move the rule to the left column.

Step 8   Use the Move Up/Move Down buttons to specify the order in which the rules apply. Highlight the desired rule, and click **Move Up** or **Move Down** to move it higher or lower in the current list.

Step 9   Click **Save** to confirm the Rogue AP rule list.

Step 10   Click **Cancel** to close the page without making any changes to the current list.

Note   To view and edit the rules applied to a controller, choose **Configure > Controller**, and click the controller name to open the controller.

Configuring and Deploying wIPS Solution

This section describes how to configure and deploy the wIPS solution using the Lifecycle theme in the Prime Infrastructure UI.

Choose **Design** > **Wireless Security** from the Lifecycle theme in the Prime Infrastructure UI. The Wireless Security wizard page appears and allows you to perform the following wIPS related configurations:

- Allows rogue policy to detect and report ad hoc networks.

- Allows rogue rules to define rules to automatically classify rogue access points.

- Allows you to add new wIPS profiles.

This section contains the following topics:

Viewing the Before You Begin Wizard Page

The Before You Begin wizard page displays information about how to use the Wireless Security wizard and includes the following information:

- Rogue Policy—The Rogue Policy page enables you to configure the rogue policy. It has three pre-configured rogue policy settings for rogue detection and containment.

- Rogue Rules—The Rogue Rules page allows you to automatically classify rogue access points based on criteria such as authentication type, matching configured SSIDs, client count, and RSSI values. Rogue rules can be created to classify rogues as Malicious and Friendly.

- wIPS Profile—The wIPS Profile page provides several pre-defined profiles from which to choose. These profiles allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. The profile can be further customized by selecting the awIPS signatures to be detected and contained.

> • Devices—The Devices page allows you to apply rogue policy, rogue rules, and wIPS profiles to controllers.

Click **Next** to configure the Rogue Policy to detect and report ad hoc networks.

Configuring Rogue Policies

This page enables you to configure the rogue policy (for access points and clients) applied to the controller.

To configure the rogue policies, follow these steps:

Step 1   Choose **Design** > **Wireless Security** > **Rogue Policy**.

Step 2   You can either set the policy settings to **Low**, **High**, or **Critical** by moving the Configure the rogue policy settings sliding bar with the mouse or select the **Custom** check box to configure the policy settings.

Step 3   In the General group box, configure the following fields:

- Rogue Location Discovery Protocol—Determines whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network. Choose one of the following from the drop-down list:

   ◦ **Disable**—Disables RLDP on all access points.

   ◦ **All APs**—Enables RLDP on all access points.

   ◦ **Monitor Mode APs**—Enables RLDP only on access points in monitor mode.

Note   With RLDP, the controller instructs a managed access point to associate with the rogue access point and sends a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points, that do not have encryption enabled.

- Expiration Timeout for Rogue AP and Rogue Client Entries—Set the expiration timeout (in seconds) for rogue access point entries. The valid range is 240 to 3600 seconds.

- Validate rogue clients against AAA—Select the **Validate rogue clients against AAA** check box to enable the AAA validation of rogue clients.

- Detect and report Adhoc networks—Select the **Detect and report Adhoc networks** check box to enable detection and reporting of rogue clients participating in ad hoc networking.

- Rogue Detection Report Interval—In the Rogue Detection Report Interval text box, enter the time interval in seconds at which the APs should send the rogue detection report to the controller. A valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.

- Rogue Detection Minimum RSSI—In the Rogue Detection Minimum RSSI text box, enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. A valid range is -70 dBM to -128 dBm. This feature is applicable to all the AP modes.

- Rogue Detection Transient Interval—In the Rogue Detection Transient Interval text box, enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only.

Step 4   In the Auto Contain group box, configure the following fields:

- Rogue on Wire—Select the **Rogue on Wire** check box to auto contain those APs that are detected on the wired network.

- Using our SSID—Select the **Using our SSID** check box.

- Valid client on Rogue AP—Select the **Valid client on Rogue AP** check box to auto contain the valid clients from connecting to the rogue APs.

- AdHoc Rogue—Select the **AdHoc Rogue** checkbox to auto contain adhoc rogue APs.

Step 5   Click **Apply** to apply the current rule to controllers. In the Devices wizard page, select the applicable controllers and click **Apply to Controllers**

Step 6   Click **Next** to configure the rogue rules.

Configuring Rogue Rules

This page enables you to define rules to automatically classify rogue access points. Prime Infrastructure applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

> **Note**   Rogue classes include the following types: Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category. Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules. Unclassified Rogue—A detected access point that does not match the Malicious or Friendly rules.

To create a new classification rule for rogue access points, follow these steps::

Step 1   Choose **Design** > **Wireless Security** > **Rogue Rules**.

Step 2   Click **Create New** to create new rogue rules.
The Add/Edit Rogue Rule window appears.

Step 3   In the General group box, configure the following fields:

- Rule Name—Enter a name for the rule in the text box.

- Rule Type—Choose **Malicious** or **Friendly** from the drop-down list.

  > **Note**   Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category. Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.

- Match Type—Choose **Match All Conditions** or **Match Any Condition** from the drop-down list.

Step 4   In the Rogue Classification Rule group box, configure the following fields:

- Open Authentication—Select the **Open Authentication** check box to enable Open Authentication.

- Match Managed AP SSID—Select the **Match Managed AP SSID** check box to enable the matching of managed AP SSID rule condition.

  Note   Managed SSID are the SSIDs configured for the WLAN and is known to the system.

- Match User Configured SSID (Enter one per line)—Select the **Match User Configured SSID** check box to enable the matching of user configured SSID rule condition.

  Note   User Configured SSID are the SSIDs that are manually added. Enter the User Configured SSIDs (one per line) in the Match User Configured SSID text box.

- Minimum RSSI—Select the **Minimum RSSI** check box to enable the Minimum RSSI threshold limit.

  Note   Enter the minimum RSSI threshold level (dB) in the text box. The detected access point is classified as malicious if it is detected above the indicated RSSI threshold.

- Time Duration—Select the **Time Duration** check box to enable the Time Duration limit.

  Note   Enter the time duration limit (in seconds) in the text box. The detected access point is classified as malicious if it is viewed for a longer period of time than the indicated time limit.

- Minimum Number Rogue Clients—Select the **Minimum Number Rogue Clients** check box to enable the Minimum Number Rogue Clients limit.

  Note   Enter the minimum number of rogue clients allowed. The detected access point is classified as malicious if the number of clients associated to the detected access point is greater than or equal to the indicated value.

Step 5   Click **Ok** to save the rule or **Cancel** to cancel the creation or changes made to the current rule.
You are returned to the Rogue Rules page and the newly added rogue rule is listed.

Step 6   Click **Apply** to apply the current rule to controllers. In the Devices wizard page, select the applicable controllers and click **Apply to Controllers**.
Note

Step 7   Click **Next** to configure the wIPS profiles.

Viewing Currently Added Rogue Rules

To view currently added rogues rules, follow these steps:

Choose **Design** > **Wireless Security** > **Rogue Rules** from the Lifecycle theme in the Prime Infrastructure UI.
The following parameters are displayed in the Rogue Rules page.

- Add Existing Rules

- Rule Name

• Rule Type

• Last Saved At

• Actions

Configuring the wIPS Profiles

Prime Infrastructure provides several pre-defined profiles from which to choose. These profiles (based on customer types, building types, industry types, and so on) allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. You can use a profile 'as is' or customize it to better meet your needs.

For more information on configuring the wIPS profile, see the section.

After configuring wIPS profile, click **Next** to open the Devices page where you can select the controllers to apply the settings.

I N D E X