



Cisco Adaptive Wireless Intrusion Prevention System Configuration Guide

Release 7.3
August 2012

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

Text Part Number: OL-23941-02

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

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

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

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

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

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

Cisco Adaptive Wireless Intrusion Prevention System Configuration Guide
Copyright © 2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface ix

CHAPTER 1

Information About wIPS	1-1
Guidelines and Limitations	1-2
wIPS in a Cisco Unified Wireless Network	1-3
wIPS Integrated Within a Cisco Unified Wireless Network	1-3
wIPS Overlay Deployment in a Cisco Unified Wireless Network	1-3
wIPS Overlay in an Autonomous or Other Wireless Network	1-5
Differences Between Controller IDS and Adaptive wIPS	1-6
Guidelines and Limitations	1-6
Reduction in False Positives	1-7
Alarm Aggregation	1-7
Forensics	1-10
Rogue Detection	1-11
Anomaly Detection	1-11
Default Configuration Profiles	1-11
Integration into Release 7.0 Features	1-11
Configuration and Administration	1-12
Adding and Deleting a Mobility Services Engine	1-12
Synchronizing Mobility Services Engines	1-12
Configuring High Availability	1-12
Configuring the Virtual Appliance	1-12
Editing Mobility Services Engine Properties	1-13
Managing Users and Groups	1-13
Configuring wIPS and Profile Management	1-13
Monitoring Capability	1-13
Provisioning MSAP Requirements	1-13
Maintenance Operations	1-14
System Compatibility	1-14

CHAPTER 2

Licensing Requirements for MSE	2-1
MSE License Structure Matrix	2-2
Sample MSE License File	2-2
Revoking and Reusing an MSE License	2-2

- Guidelines and Limitations 2-3
- Adding a Mobility Services Engine to the Prime Infrastructure 2-4
 - Deleting an MSE License File 2-7
 - Deleting a Mobility Services Engine from the Prime Infrastructure 2-7
- Registering Device and wIPS Product Authorization Keys 2-8
- Installing Device and wIPS License Files 2-12
- Registering Tag PAKs 2-12
- Installing Tag Licenses 2-13

CHAPTER 3

- Information About Synchronizing the Prime Infrastructure and Mobility Services Engines 3-1
- Prerequisites for Synchronizing the Mobility Services Engine 3-2
- Working with Third-Party Elements 3-2
 - Deleting Elements or Marking Them as Third-Party Elements 3-2
- Synchronizing Controllers with a Mobility Services Engine 3-3
 - Synchronizing a Controller, Catalyst Switch, or Event Group 3-3
 - Assigning an MSE to the Controller 3-4
 - Unassigning a Network Design, Controller, Wired Switch, or Event Group from the MSE 3-5
- Configuring Automatic Database Synchronization and Out-of-Sync Alerts 3-5
 - Configuring Automatic Database Synchronization 3-6
 - Smart Controller Assignment and Selection Scenarios 3-7
 - Out-of-Sync Alarms 3-7
- Viewing Mobility Services Engine Synchronization Status 3-7
 - Viewing Mobility Services Engine Synchronization Status 3-8
 - Viewing Synchronization History 3-8

CHAPTER 4

- Overview to the High Availability Architecture 4-1
- Pairing Matrix 4-2
- Guidelines and Limitations for High Availability 4-2
- Failover Scenario for High Availability 4-2
- Failback 4-3
- HA Licensing 4-3
- Configuring High Availability on the MSE 4-3
- Viewing Configured Parameters for High Availability 4-6
- Viewing High Availability Status 4-7

CHAPTER 5

- Physical Appliance 5-1

Virtual Appliance	5-1
Operating Systems Requirements	5-2
Client Requirements	5-2
Prerequisites for Setting Up an MSE Virtual Appliance on a Server	5-3
Virtual Appliance Sizing	5-3
Reinstalling the MSE on a Physical Appliance	5-3
Deploying the MSE Virtual Appliance	5-4
Adding a Virtual Appliance License to the Prime Infrastructure	5-8
Viewing the MSE License Information Using the License Center	5-9
Removing a License File Using the License Center	5-9

CHAPTER 6

Licensing Requirement	6-1
Editing General Properties and Viewing Performance	6-1
Editing General Properties	6-2
Viewing Performance Information	6-4
Viewing Active Sessions on a System	6-5
Adding and Deleting Trap Destinations	6-6
Adding Trap Destinations	6-6
Deleting Trap Destinations	6-7
Viewing and Configuring Advanced Parameters	6-7
Viewing Advanced Parameter Settings	6-8
Initiating Advanced Parameters	6-8
Configuring Advanced Parameters	6-9
Initiating Advanced Commands	6-10

CHAPTER 7

Prerequisites	7-1
Guidelines and Limitations	7-1
Managing User Groups	7-1
Adding User Groups	7-1
Deleting User Groups	7-2
Changing User Group Permissions	7-2
Managing Users	7-3
Adding Users	7-3
Deleting Users	7-3
Changing User Properties	7-4

CHAPTER 8

Guidelines and Limitations	8-1
Prerequisites	8-1

Information About wIPS Configuration and Profile Management	8-2
Guidelines and Limitations	8-2
Configuring Access Points for wIPS Monitor Mode	8-2
Configuring wIPS Profiles	8-4
<hr/>	
CHAPTER 9	
Working with Alarms	9-1
Guidelines and Limitations	9-1
Viewing Alarms	9-2
Viewing the MSE Alarm Details	9-2
Assigning and Unassigning Alarms	9-4
Deleting and Clearing Alarms	9-5
E-mailing Alarm Notifications	9-5
Working with Events	9-6
Displaying Location Notification Events	9-6
Working with Logs	9-6
Guidelines and Limitations	9-6
Configuring Logging Options	9-7
MAC Address-based Logging	9-8
Downloading Log Files	9-8
Generating Reports	9-8
MSE Analytics	9-9
Client Location	9-9
Client Location Density	9-11
Device Count by Zone	9-13
Device Dwell Time by Zone	9-14
Guest Location Density	9-16
Location Notifications by Zone	9-17
Mobile MAC Statistics	9-19
Rogue AP Location Density	9-20
Creating a Device Utilization Report	9-22
Security Reports and Alarms for wIPS	9-25
Creating a New wIPS Security or Alarms Report	9-25
Viewing a Saved wIPS Report	9-27
Viewing Scheduled wIPS Report Runs	9-27
Client Support on the MSE	9-27
Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address	9-28
Viewing the Clients Detected by the MSE	9-29
Configuring Buildings	9-34
Monitoring Geo-Location	9-40

Adding a GPS Marker to a Floor Map	9-40
Editing a GPS Marker	9-41
Deleting a GPS Marker Present on a Floor	9-41

CHAPTER 10

Licensing for MSAP	10-1
Provisioning MSAP Service Advertisements	10-2
Adding Service Advertisements to the Floor Map	10-3
Creating Service Advertisements from the Floor Map	10-4
Deleting Service Advertisements	10-4
Applying Service Advertisements to a Venue	10-4
Viewing the Configured Service Advertisements per MSE	10-5
Viewing the MSE Summary Page for MSAP License Information	10-6
Viewing Service Advertisements Synchronization Status	10-6
MSAP Reports	10-6

CHAPTER 11

Guidelines and Limitations	11-1
Recovering a Lost Password	11-1
Recovering a Lost Root Password	11-2
Backing Up and Restoring Mobility Services Engine Data	11-2
Guidelines and Limitations	11-2
Backing Up Mobility Services Engine Historical Data	11-3
Restoring Mobility Services Engine Historical Data	11-3
Enabling Automatic Location Data Backup	11-4
Downloading Software to the Mobility Services Engines	11-4
Manually Downloading Software	11-5
Configuring the NTP Server	11-6
Resetting the System	11-6
Clearing the Configuration File	11-6

APPENDIX 12

wIPS Policy Alarm Encyclopedia	12-1
Security IDS/IPS Overview	12-1
Intrusion Detection—Denial of Service Attack	12-2
Denial of Service Attacks Against Access Points	12-3
Denial of Service Attack Against Infrastructure	12-8
Denial of Service Attacks Against Client Station	12-13
Intrusion Detection—Security Penetration	12-23

APPENDIX N

Rogue Management N-1

- Rogue Access Point Challenges **N-1**
- Rogue Access Point Location, Tagging, and Containment **N-1**
 - Detecting and Locating Rogue Access Points **N-2**
- Monitoring Alarms **N-3**
 - Monitoring Rogue Access Point Alarms **N-3**
 - Monitoring Rogue Ad hoc Alarms **N-7**
 - Configuring Auto Switch Port Tracing Criteria on the Prime Infrastructure **N-11**
- Configuring Controllers **N-12**
 - Configuring Rogue Policies **N-13**
 - Configuring Rogue AP Rules **N-13**
- Configuring Controller Templates **N-13**
 - Configuring Rogue Policies **N-14**
 - Configuring Rogue AP Rules **N-15**

APPENDIX O

- RRM Dashboard **0-1**
 - Channel Change Notifications **0-2**
 - Transmission Power Change Notifications **0-3**
 - RF Grouping Notifications **0-3**
 - Viewing the RRM Dashboard **0-3**
- Configuring Controllers **0-4**
 - Configuring an RRM Threshold Controller (for 802.11a/n or 802.11b/g/n) **0-5**
 - Configuring 40-MHz Channel Bonding **0-5**
- Configuring Controller Templates **0-6**
 - Configuring an RRM Threshold Template for 802.11a/n or 802.11b/g/n **0-6**
 - Configuring an RRM Interval Template (for 802.11a/n or 802.11b/g/n) **0-7**



Preface

This preface introduces the *Cisco Adaptive Wireless Intrusion Prevention System* and contains the following sections:

- [Objectives, page ix](#)
- [Audience, page ix](#)
- [Conventions, page ix](#)
- [Related Documentation, page x](#)
- [Obtaining Documentation and Submitting a Service Request, page x](#)

Objectives

This guide describes how to use the Cisco Prime Infrastructure to configure and manage the Cisco 3300 series mobility services engine and the Context-Aware Service, that resides on the mobility services engine.

Audience

The purpose of this guide is to help you configure and manage wIPS. Before you begin, you should be familiar with network structures, terms, and concepts.

Conventions

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

- Commands and keywords appear in **boldface**.
- *Italics* indicate arguments for which you supply values.
- Series of menu options appear as **option > option**.

Examples use the following conventions:

- Examples depict page displays and the command line in *screen* font.
- Information you need to enter in examples is shown in **bold screen** font.
- Variables for which you must supply a value are shown in *italic screen* font.

**Note**

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

**Tip**

Means the following information will help you solve a problem.

**Caution**

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

Related Documentation

See the *Cisco 3310 Mobility Services Engine Getting Started Guide* or *Cisco 3500 Mobility Services Engine Getting Started guide* for mobility services engine installation and setup information.

This document is available on Cisco.com at the following URL:

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

Obtaining Documentation and Submitting a Service Request

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

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

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



CHAPTER 1

Overview

This chapter describes the role of the Cisco 3300 mobility services engine (MSE) and the Cisco Adaptive Wireless Intrusion Prevention System (wIPS) within the overall Cisco Unified Wireless Network (CUWN). This chapter contains the following sections:

- [Information About wIPS, page 1-1](#)
- [wIPS in a Cisco Unified Wireless Network, page 1-3](#)
- [Differences Between Controller IDS and Adaptive wIPS, page 1-6](#)

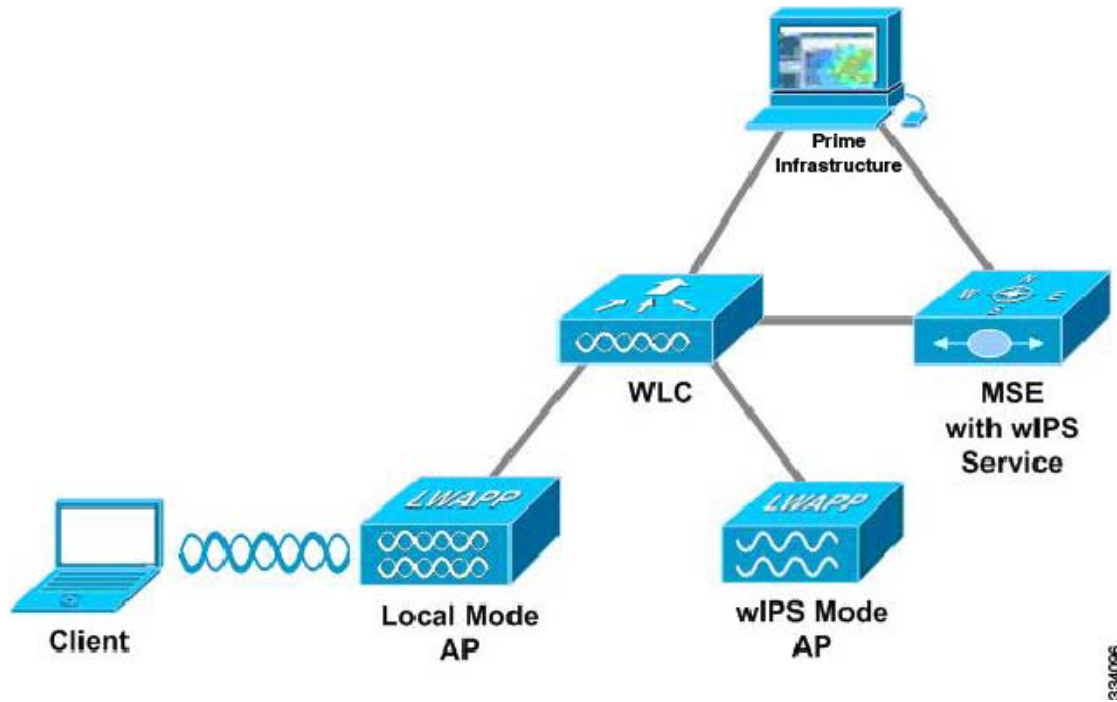
Information About wIPS

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

Built on 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 enabled access points. Alarm information and forensic files are stored on the mobility services engine for archival purposes.
- A wIPS monitor mode access point—Provides constant channel scanning with attack detection and forensics (packet capture) capabilities.
- Local mode access point—Provides wireless service to clients in addition to time-sliced rogue scanning.
- Wireless LAN Controller—Forwards attack information received from wIPS enabled access points to the mobility services engine and distributes configuration parameters to access points.
- Cisco Prime Network Control System (NCS)—Provides a centralized management platform for the administrator to configure the wIPS Service on the mobility services engine, push wIPS configurations to the controller, and configure access points in wIPS monitor mode. NCS is also used to view wIPS alarms, forensics, reporting, and to access the attack encyclopedia (see [Figure 1-1](#)).

Figure 1-1 Wireless Intrusion Prevention System



Communication among the system components involves the following protocols:

- Control and Provisioning of Wireless Access Points (CAPWAP)—This protocol is the successor to LWAPP and is used for communication between access points and controllers. It provides a bi-directional tunnel in which alarm information is sent to the controller and configuration information is sent to the access point.
- Network Mobility Services Protocol (NMSP)—The protocol handles communication between controllers and the mobility services engine. In 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.

Guidelines and Limitations

The HREAP mode access points support wIPS.

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).

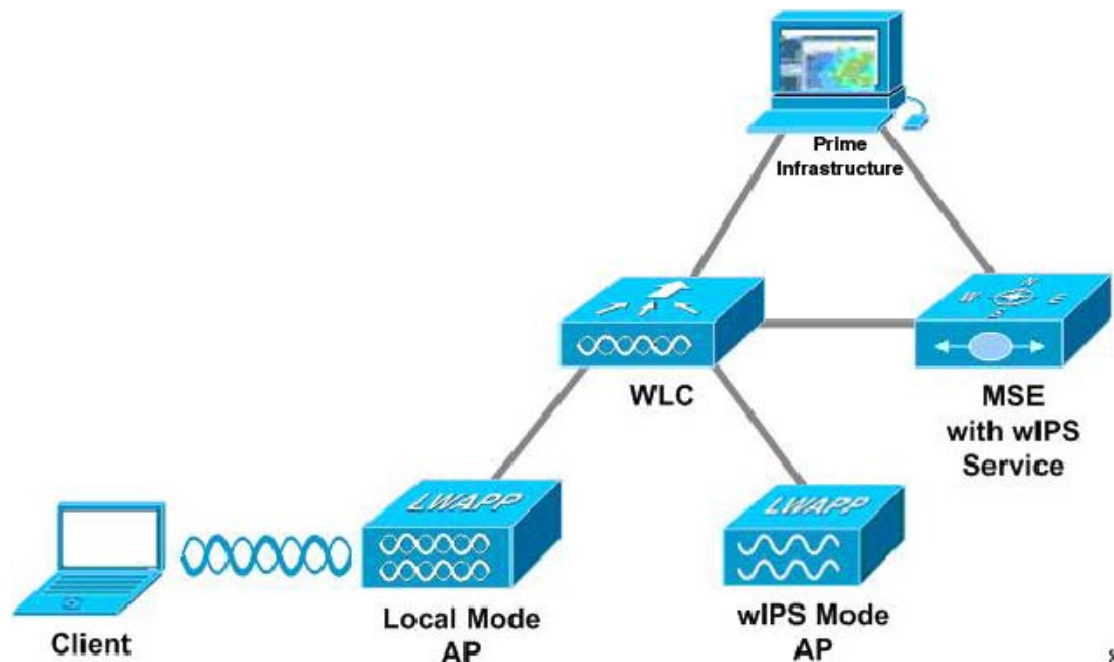
This section contains the following topics:

- [wIPS Integrated Within a Cisco Unified Wireless Network, page 1-3](#)
- [wIPS Overlay Deployment in a Cisco Unified Wireless Network, page 1-3](#)
- [wIPS Overlay in an Autonomous or Other Wireless Network, page 1-5](#)

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 NCS. We recommend this configuration because it allows the tightest integration between the client serving and monitoring infrastructure (See [Figure 1-2](#)).

Figure 1-2 wIPS Integrated Within CUWN



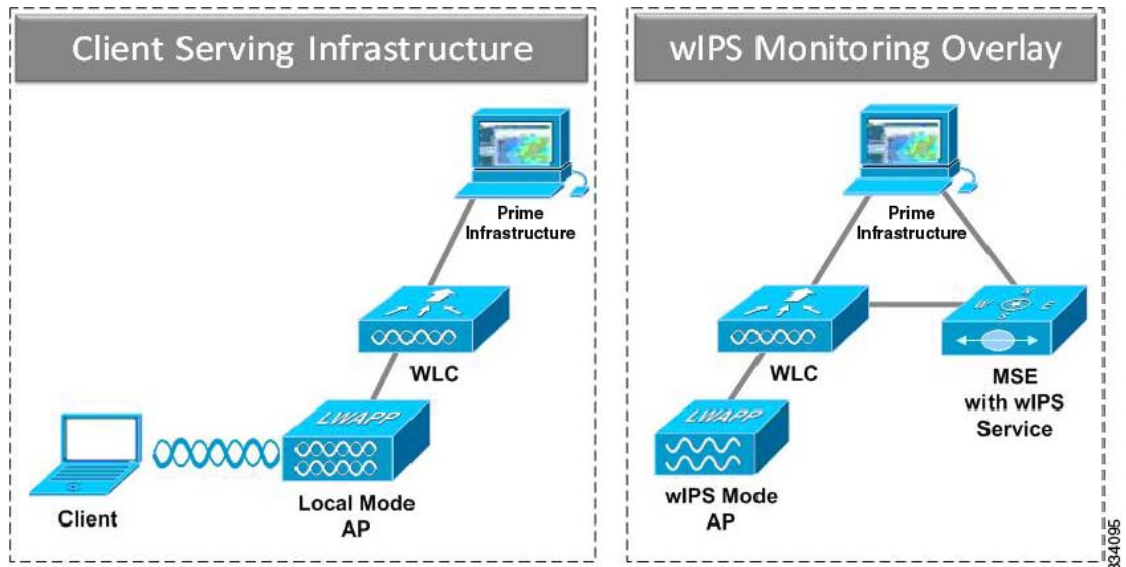
934096

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

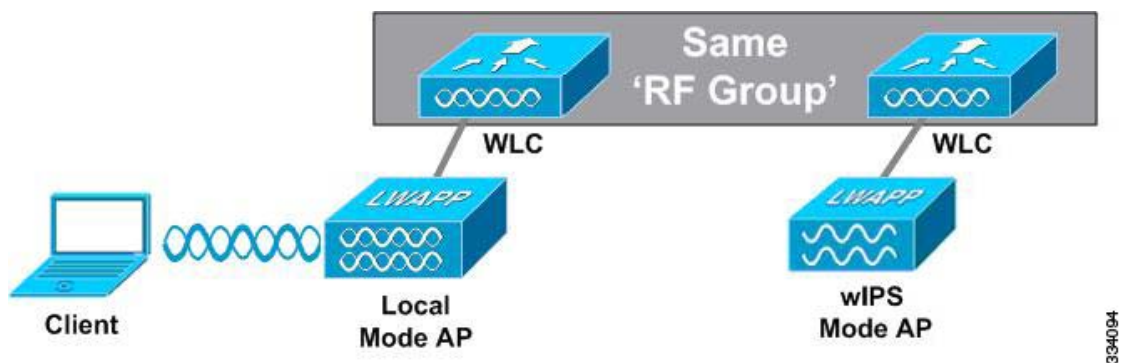
require distinct network infrastructure and security infrastructure systems with separate management consoles (Figure 1-3). This deployment model is also used when the total number of access points (wIPS monitor and local mode) exceed the 3000 access point limit contained in the Prime Infrastructure.

Figure 1-3 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 items must be completed. The wIPS system operates on the 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 1-4).

Figure 1-4 Controllers 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 NCS instance.
- Management Frame Protection (MFP) alarms are only shown on the client infrastructure NCS instance.
- Rogue alarms are shown in both NCS instances.

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

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

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

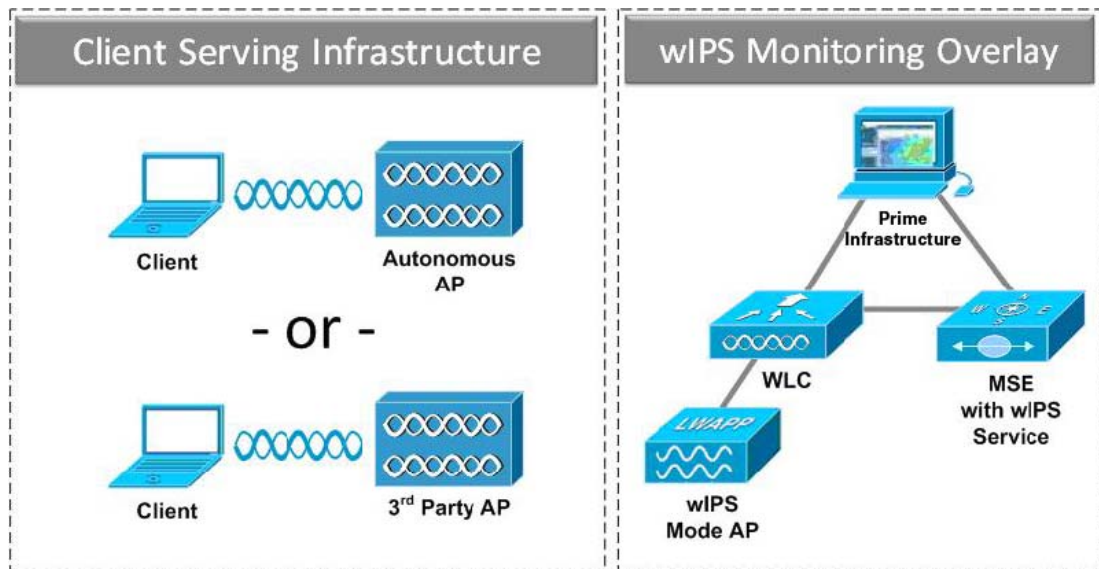
	Client Serving Prime Infrastructure	wIPS Monitoring Overlay Prime Infrastructure
wIPS alarms	No	Yes
MFP alarms	Yes	No
Rogue alarms	Yes	Yes
Rogue location	High accuracy	Low accuracy
Rogue containment	Yes	Yes, but scalable

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 Adaptive 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 (Figure 1-5).

Figure 1-5 wIPS Overlay in Autonomous



334093

Differences Between Controller IDS and Adaptive wIPS

This section contains the following topics:

- [Guidelines and Limitations, page 1-6](#)
- [Reduction in False Positives, page 1-7](#)
- [Alarm Aggregation, page 1-7](#)
- [Forensics, page 1-10](#)
- [Rogue Detection, page 1-11](#)
- [Anomaly Detection, page 1-11](#)
- [Default Configuration Profiles, page 1-11](#)
- [Integration into Release 7.0 Features, page 1-11](#)

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.

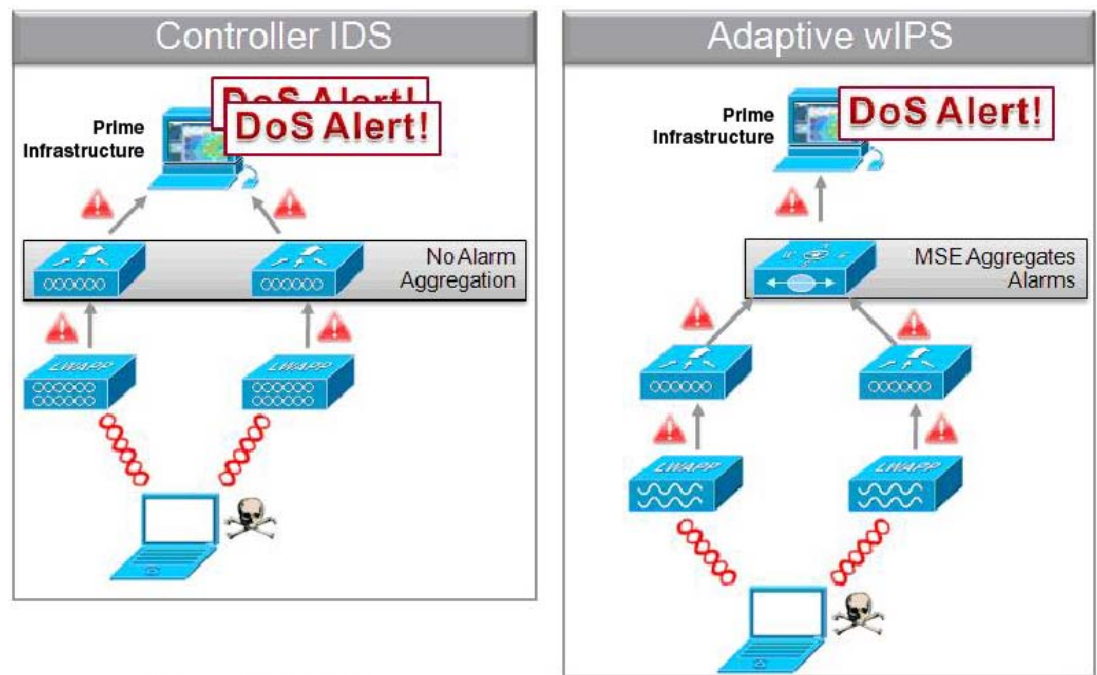
Reduction in False Positives

The wIPS facilitates a reduction in false positives with respect to security monitoring of the wireless network. In contrast to the controller-based solution of Cisco, which triggers an alarm when it detects a number of management frames over the air, wIPS only triggers an alarm when it detects a number of management frames over the air that are causing damage to the wireless infrastructure network. This 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. Only when attacks are launched against the infrastructure are alarms raised.

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 (Figure 1-6).

Figure 1-6 Alarm Aggregation Using Cisco Controller-based IDS Versus Adaptive 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 Table 1-2 and Table 1-3, 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:

- [DoS Attacks, page 1-8.](#)
- [Security Penetration Attacks, page 1-8](#)
- [wIPS Alarm Flow, page 1-9](#)

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. [Table 1-2](#) compares the DoS attacks detected by the controller-based IDS and WIPS service.

Table 1-2 DoS Attack Detection by Controller IDS and WIPS

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

Security Penetration Attacks

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

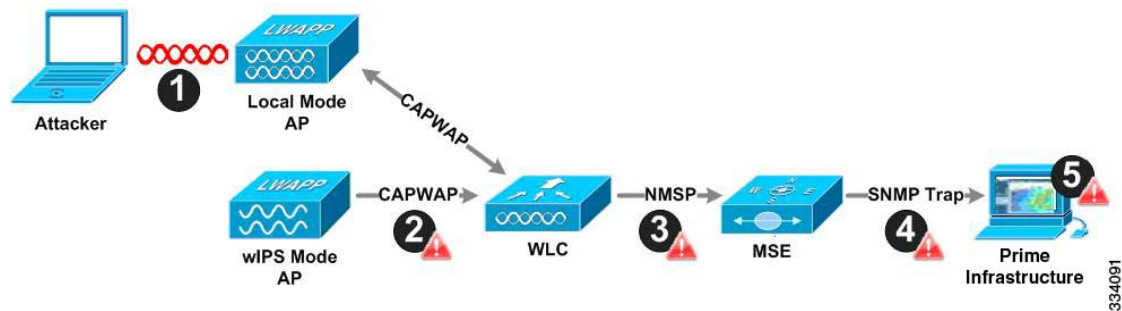
Table 1-3 Security Penetration Attack Detection by Controller IDS and wIPS

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

wIPS Alarm Flow

The Adaptive wIPS system follows a linear chain of communication to propagate attack information obtained from initially scanning the airwaves to forwarding information to the Prime Infrastructure (see [Figure 1-7](#)).

Figure 1-7 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 Network Mobility Service Protocol (NMSP).
4. Once received by the wIPS service on the mobility services engine, the alarm update is added to the alarm database for archival and attack tracking. An SNMP trap is forwarded to 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.

Forensics

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

**Note**

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.

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%, 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 preexisting signature in the wIPS system.

Default Configuration Profiles

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

Integration into Release 7.0 Features

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

Configuration and Administration

You can use the Prime Infrastructure to perform different configuration and administrative tasks, including adding and removing a mobility services engine, configuring mobility services engine properties, and managing users and groups.

This section contains the following topics:

- [Adding and Deleting a Mobility Services Engine, page 1-12](#)
- [Synchronizing Mobility Services Engines, page 1-12](#)
- [Configuring High Availability, page 1-12](#)
- [Configuring the Virtual Appliance, page 1-12](#)
- [Editing Mobility Services Engine Properties, page 1-13](#)
- [Synchronizing Mobility Services Engines, page 1-12](#)
- [Monitoring Capability, page 1-13](#)
- [Provisioning MSAP Requirements, page 1-13](#)
- [Maintenance Operations, page 1-14](#)
- [System Compatibility, page 1-14](#)

Adding and Deleting a Mobility Services Engine

You can use the Prime Infrastructure to add and delete a mobility services engine within the network. You can also define the service supported on the mobility services engine. See [Chapter 2, “Adding and Deleting Mobility Services Engines and Licenses,”](#) for configuration details.

Synchronizing Mobility Services Engines

You can use the Prime Infrastructure to synchronize Cisco wireless LAN controllers and the Prime Infrastructure with mobility services engines. See [Chapter 3, “Synchronizing Mobility Services Engines,”](#) for more information.

Configuring High Availability

You can use the Prime Infrastructure to configure high availability on the MSE. The mobility services engine is a platform for hosting multiple mobility applications. Every active MSE is backed up by another inactive instance. The active MSE is called the primary MSE and the inactive MSE is called the secondary MSE. See [Chapter 4, “Configuring High Availability,”](#) for more information.

Configuring the Virtual Appliance

The MSE comes preinstalled on a physical appliance with various performance characters. The MSE is delivered in two modes, the physical appliance and the virtual appliance. See [Chapter 5, “MSE Delivery Modes,”](#) for more information.

Editing Mobility Services Engine Properties

You can use the Prime Infrastructure to configure the following parameters on the mobility services engine. See [Chapter 6, “Configuring and Viewing System Properties,”](#) for configuration details.

- **General Properties**—Enables you to assign a contact name, username, password, and HTTP for the mobility services engine.
- **Active Sessions**—Enables you to view active user sessions on the mobility services engine.
- **Trap Destinations**—Enables you to specify which NCS or Cisco Security Monitoring, Analysis and Response System (CS-MARS) network management platform is the recipient of SNMP traps generated by the mobility services engine.
- **Advanced Parameters**—Enables you to set the number of days to keep events, reboot hardware, shut down hardware, or clear the database.

Managing Users and Groups

You can use the Prime Infrastructure to manage users, groups, and host access on the mobility services engine. See [Chapter 7, “Managing Users and Groups,”](#) for configuration details.

Configuring wIPS and Profile Management

You can use the Prime Infrastructure to configure the Cisco Adaptive wIPs service. See the [“Configuring wIPS Profiles”](#) section on page 8-4 for more information.

Monitoring Capability

You can use the Prime Infrastructure to monitor alarms, events, and logs generated by mobility services engine. You can also monitor the status of mobility services engines, clients, interferers, and tagged assets. Additionally, you can generate a utilization report for the mobility services engine to determine CPU and memory utilization as well as counts for clients, tags and rogue access points and clients. See [Chapter 9, “Monitoring the System and Services,”](#) for more information.

Provisioning MSAP Requirements

Cisco Mobility Services Advertisement Protocol (MSAP) provides requirements for MSAP client and server and describes the message exchanges between them. Mobile devices can retrieve service advertisements from MSAP server over Wi-Fi infrastructure using MSAP. MSAP is introduced in this release in the Mobility Services Engine (MSE) and provides server functionality. See [Chapter 10, “MSAP,”](#) for more information.

Maintenance Operations

You can back up mobility services engine data to a predefined FTP folder on the Prime Infrastructure at defined intervals, and restore the mobility services engine data from that NCS. Other mobility services engine maintenance operations that you can perform include downloading new software images to all associated mobility services engines from any NCS station, and clearing mobility services engine configurations. See [Chapter 11, “Performing Maintenance Operations,”](#) for more information.

**Note**

Details on recovering GRUB and root passwords for the mobility services engine using the command-line interface (rather than the Prime Infrastructure) are also addressed in [Chapter 11, “Performing Maintenance Operations”](#).

System Compatibility

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



CHAPTER 2

Adding and Deleting Mobility Services Engines and Licenses

This chapter describes how to add and delete a Cisco 3300 series mobility services engine to and from the Cisco Prime Infrastructure.



Note

The Mobility Services Engines, Synchronize Services, Synchronization History, High Availability, Context Aware Notifications, and MSAP pages on the Services tab are available only in the virtual domain in Release 7.3.

This chapter contains the following sections:

- [Licensing Requirements for MSE, page 2-1](#)
- [Guidelines and Limitations, page 2-3](#)
- [Adding a Mobility Services Engine to the Prime Infrastructure, page 2-4](#)
- [Deleting a Mobility Services Engine from the Prime Infrastructure, page 2-7](#)
- [Registering Device and wIPS Product Authorization Keys, page 2-8](#)
- [Installing Device and wIPS License Files, page 2-12](#)
- [Registering Tag PAKs, page 2-12](#)
- [Installing Tag Licenses, page 2-13](#)

Licensing Requirements for MSE

The MSE packages together multiple product features related to network topology, design such as NMSP, and Network Repository along with related service engines and application processes, such as the following:

- Location Service or Context-Aware Service software
- Wireless Intrusion Prevention System (wIPS)

To enable smooth management of MSE and its services, various licenses are offered.

This section contains the following topics:

- [MSE License Structure Matrix, page 2-2](#)
- [Sample MSE License File, page 2-2](#)

- [Revoking and Reusing an MSE License, page 2-2](#)

MSE License Structure Matrix

Table 2-1 lists the breakup of the licenses between the high-end, low-end, and evaluation licenses for the MSE, Location services or Context-Aware Service software, and wIPS.

Table 2-1 MSE License Structure Matrix

	High End	Low End	Evaluation
MSE Platform	High-end appliance and infrastructure platform.	Low-end appliance and infrastructure platform.	60 days.
Location Service or Context-Aware Service Software	3000, 6000, 12,000 tags	1000 tags	60 days, 100 tags and 100 elements.
	3000, 6000, 12,000 elements	1000 elements	
wIPS	5000 access points	2000 access points	60 days, 20 access points.

Sample MSE License File

The following is a sample MSE license file:

```
FEATURE MSE cisco 1.0 permanent uncounted \
    VENDOR_STRING=UDI=udi,COUNT=1 \
    HOSTID=ANY \
    NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</LicLineID> \
    <PAK>dummyPak</PAK>" \
    SIGN="0C04 1EBA BE34 F208 404F 98ED 43EC \
    45D7 F881 08F6 7FA5 4DED 43BC AF5C C359 0444 36B2 45CF 6EA6 \
    1DB1 899F 413F F543 F426 B055 4C7A D95D 2139 191F 04DE"
```

This sample file has 5 license entries. The first word of the first line of any license entry tells you what type of license it is. It can either be a Feature or Increment license. A Feature license is a static, lone-item license. There can be multiple service engines running in the MSE. An Increment license is an additive license. In the MSE, the individual service engines are treated as Increment licenses.

The second word of the first line defines the specific component to be licensed. 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 rehosed.

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 Network Control System Configuration Guide, Release 7.3*.

Revoking an MSE License Using the MSE CLI

You can also revoke an MSE license from the MSE command-line interface manually without using the Prime Infrastructure.

To revoke an MSE license using the MSE command-line interface, follow these steps:

-
- Step 1** Log in to an MSE using command-line interface.
- Step 2** Navigate to `/opt/mse/licensing/`
- Step 3** Delete the license file by entering the following command:
- ```
rm /opt/mse/licensing/license file name.lic
```
- where *license file name* is the name of the license file.
- Step 4** Restart the MSE process by entering the following command:
- ```
/etc/init.d/mseed restart
```
- The MSE license is revoked.
-

Guidelines and Limitations

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

- A mobility services engine can support multiple services.
- After adding a new mobility services engine, you can synchronize network designs (campus, building, and outdoor maps), controllers, switches (Catalyst 3000 series and 4000 series only), and event groups for the mobility services engine and the Prime Infrastructure.
- Tag PAKs are registered with AeroScout only if AeroScout engine for tags was selected during the addition of an MSE. This procedure is not necessary if Cisco tag engine was selected as the Cisco license is shared between all devices including the tags.
- If you had changed the username and password during the automatic installation script, enter those values here while adding a mobility services engine 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.



Tip

To learn more about Cisco Adaptive wIPS features and functionality, go to Cisco.com to watch a multimedia presentation. Here you can find the learning modules for a variety of 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.

To add a mobility services engine to the Prime Infrastructure, log into the Prime Infrastructure and follow these steps:



Note

The **Services > Mobility Services Engine** page is available only in the virtual domain in Release 7.3.

- Step 1** Verify that you can ping the mobility services engine.
- Step 2** Choose **Services > Mobility Services** to display the Mobility Services page.
- Step 3** From the Select a command drop-down list, choose **Add Mobility Services Engine**. Click **Go**.
- Step 4** In the Device Name text box, enter a name for the mobility services engine.
- Step 5** In the IP Address text box, enter the IP address of the mobility services engine.
- Step 6** (Optional) In the Contact Name text box, enter the name of the mobility services engine administrator.
- Step 7** In the User Name and Password text boxes, enter the username and password for the mobility services engine.

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 **HTTP** check box to allow communication between the mobility services engine and third-party applications. By default, the Prime Infrastructure uses HTTPs to communicate with MSE.
- Step 9** Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the mobility services engine.

This option is applicable for network designs, wired switches, controllers and event definitions. The existing location history data is retained, however, you must use manual service assignments to perform any future location calculations.

Step 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 either of the following engines to track tags:

- Cisco Tag Engine
- or
- Partner Tag Engine

Step 12 Click **Save**.



Note See [Chapter 3, “Synchronizing Mobility Services Engines”](#).



Note After adding a new mobility services engine, you can synchronize network designs (campus, building, and outdoor maps), controllers, switches (Catalyst Series 3000 only), and event groups on the local mobility services engine using the Prime Infrastructure. You can perform this synchronization immediately after adding a new mobility services engine or at a later time. To synchronize the local and the Prime Infrastructure databases, see [Chapter 3, “Synchronizing Mobility Services Engines”](#).

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 mobility services engine, 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 either of the following engines to track tags:
 - Cisco Context-Aware Engine for Clients and Tags
 - Partner Tag Engine



Note By default, the Context Aware Service check box and Cisco Context-Aware Engine for Clients and Tags radio button are enabled.

- Wireless Intrusion Prevention System—If you select the Wireless Intrusion Prevention System check box, it detects wireless and performance threats.
- MSAP Service—If you select the MSAP Service check box, it provides service advertisements that describe the available services for the mobile devices.



Note With MSE 6.0 and later, you can enable multiple services (CAS and wIPS) simultaneously. Before Version 6.0, mobility services engines only supported one active service at a time.

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

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.

- 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 controllers 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** Click **Device Name** to delete a license file for a particular service.
- Step 3** From the Select a command drop-down list, choose **Edit Configuration**. The Edit Mobility Services Engine dialog box appears.
- Step 4** Click **Next** in the Edit Mobility Services Engine dialog box. The MSE License Summary page appears.
- Step 5** Choose the MSE license file that you want to delete in the MSE License Summary page.
- Step 6** Click **Remove License**.
- Step 7** Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the license.
- Step 8** Click **Next** to enable services on the mobility services engine.

Deleting a Mobility Services Engine from the Prime Infrastructure

To delete one or more mobility services engines from the Prime Infrastructure database, follow these steps:

**Note**

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

-
- Step 1** Choose **Services > Mobility Services**.
The Mobility Services page appears.
- Step 2** Select the mobility services engine 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 mobility services engine 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.

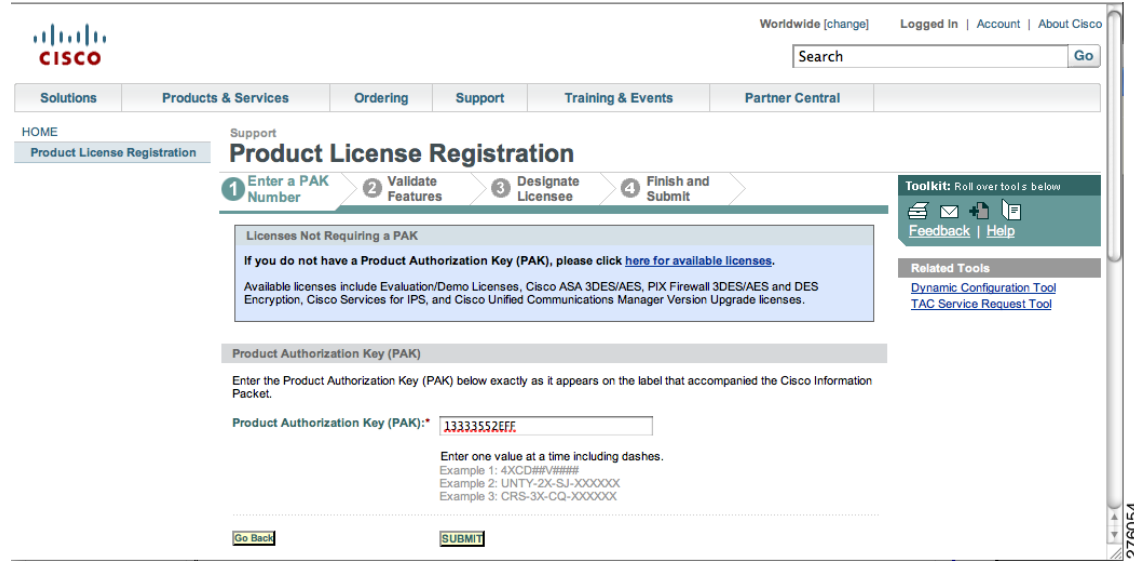
**Note**

See the “[Registering Tag PAKs](#)” section on page 2-12 for more information.

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

- Step 1** On your web browser, go to <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet>.
- Step 2** Enter the PAK, and click **SUBMIT** (see [Figure 2-1](#)).

Figure 2-1 Enter PAK Number Page



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



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

Figure 2-2 Validate Features Page

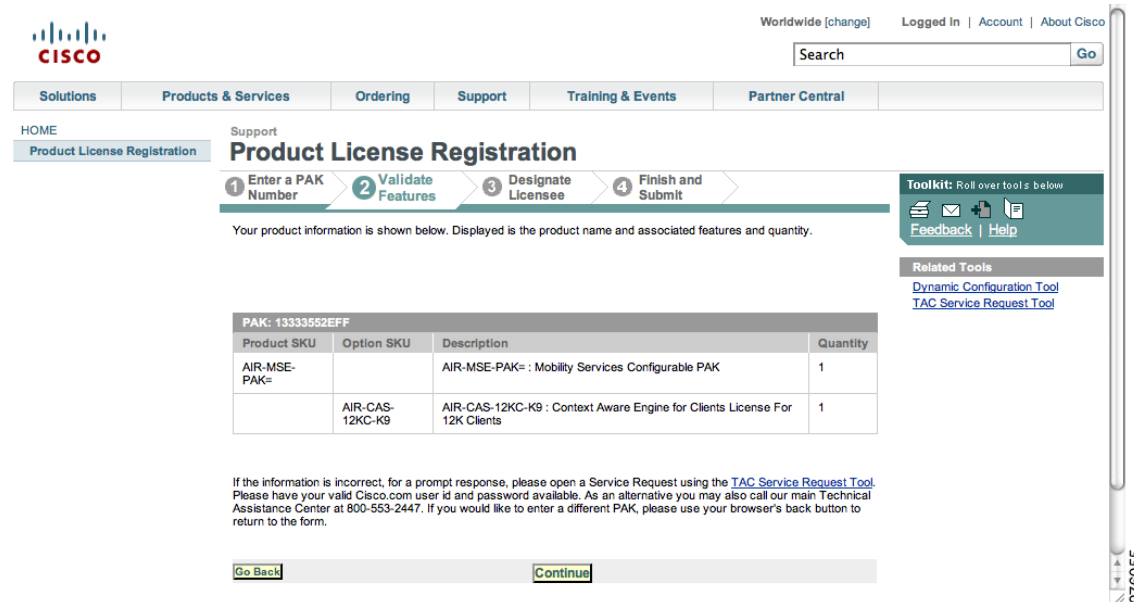


Figure 2-3 Designate Licensee, Page 1 of 2

Worldwide [change] Logged In | Account | About Cisco

Search Go

Solutions Products & Services Ordering Support Training & Events Partner Central

HOME

Product License Registration

Support

Product License Registration

1 Enter a PAK Number 2 Validate Features 3 Designate Licensee 4 Finish and Submit

Mobility Services Engine

Toolkit: Roll over tools below

Feedback | Help

Related Tools

Dynamic Configuration Tool
TAC Service Request Tool

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

A *** denotes a required field

About your License Key

Please enter below the UDI of the MSE appliance that you will be installing your software on. You will be installing your software on. The UDI information will be sent via email within 1 hour to the email address specified.

Host Id*

AIR-MSE-3350-K9-V01:MXQ821A31P

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

Agreement:* Click here if you accept the conditions of the [End-User License Agreement](#)

- Step 4** In the Designate Licensee page, enter the UDI of the mobility services engine in the Host Id text box. This is the mobility services engine on which the license is installed.



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

- Step 5** Select the **Agreement** check box. Registrant information appears beneath the Agreement check box (see Figure 2-4).

Figure 2-4 Designate Licensee, Page 2 of 2

Registrant Information

Name:* First Name:* Last Name:*
username1 username2

Company:* CISCO SYSTEMS

Title
Technical Writer

Address1:* 3550 Cisco Way

Address2

City/Town:* State/Prov:* Postal/Zip:*
San Jose CA 95134

Country:*
USA

Phone:* 1408551234

Fax

Email:* username1@example.com

Modify the information as necessary.

- 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 (see [Figure 2-5](#)).

Figure 2-5 *Finish and Submit Page*

HOME
Product License Registration

Support
Product License Registration

1 Enter a PAK Number 2 Validate Features 3 Designate Licensee 4 Finish and Submit

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

Licensee Information

Registrant Profile
[Edit Details](#)

Full Name: username1
Job Title: Technical Writer
Company: CISCO SYSTEMS
Business Address: 3550 Cisco Way
San Jose, CA 95134
USA
Phone: 14085551234
Fax:
Email: username1@example.com

End User Profile
[Edit Details](#)

Full Name: username1
Job Title: Technical Writer
Company: CISCO SYSTEMS
Business Address: 3550 Cisco Way
San Jose, CA 95134
USA
Phone: 14085551234
Fax:
Email: username1@example.com

Toolkit: Roll over tools below
Feedback | Help

Related Tools
[Dynamic Configuration Tool](#)
[TAC Service Request Tool](#)

276059

- Step 8** In the Finish and Submit page, review the registrant and end-user data. Click **Edit Details** to correct any information. Click **Submit**. A confirmation page appears (see [Figure 2-6](#)).

Figure 2-6 *Registration Confirmation Page*

Worldwide [change] Logged In | Account | About Cisco

Search Go

Solutions Products & Services Ordering Support Training & Events Partner Central

HOME
Product License Registration

Support
Product License Registration

Registration Complete

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

Toolkit: Roll over tools below
Feedback | Help

Related Tools
[Dynamic Configuration Tool](#)
[TAC Service Request Tool](#)

276060

Installing Device and wIPS License Files

You can install client and wIPS licenses from the Prime Infrastructure.


Note

The tag license installation is separate only if the AeroScout engine was selected for tag calculation while adding the MSE.


Note

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

Tag licenses are installed using the AeroScout System Manager. See the [“Installing Tag Licenses” section on page 2-13](#) for more information.

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

-
- Step 1** Choose **Administration > License Center**.
 - 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 you entered when registering the PAK.

- Step 5** Click **Choose File** to browse to and select the license file.
 - Step 6** Click **Upload**. The newly added license appears in the MSE license file list.
-

Registering Tag PAKs

To register tags at the AeroScout website, follow these steps:

-
- Step 1** On your web browser, go to the website of AeroScout and open the Support page.
 - Step 2** Log in if you have an existing account, or click **Create New Account** to create a log in, username, and password.
If you created a new account, you receive a notification e-mail with your username and password.
 - Step 3** After logging in, click **Register Products Purchased from Cisco** on the Home tab.
To register your product, you need the following information: PAK number, MSE ID (MSE serial number (S/N)), and Installation Type.
You receive an e-mail message from AeroScout that confirms the registration.
Your PAK number is verified within two business days by e-mail. If your PAK number is found to be invalid, you must register again with a valid PAK number.
-

Installing Tag Licenses

After successfully registering your PAK, you receive an e-mail with your license key and instructions on how to download Context-Aware Service software and a copy of the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide*.

See the *AeroScout Context-Aware for Tags, for Cisco Mobility Services Engine Users Guide* for details on installing your tag licenses on the Aeroscout's Support website.



CHAPTER 3

Synchronizing Mobility Services Engines

This chapter describes how to synchronize Cisco wireless LAN controllers and the Cisco Prime Infrastructure with 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.

This chapter contains the following sections:

- [Information About Synchronizing the Prime Infrastructure and Mobility Services Engines, page 3-1](#)
- [Synchronizing Controllers with a Mobility Services Engine, page 3-3](#)
- [Configuring Automatic Database Synchronization and Out-of-Sync Alerts, page 3-5](#)
- [Viewing Mobility Services Engine Synchronization Status, page 3-7](#)

Information About 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.

After adding a mobility services engine 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 mobility services engine.

- **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.
- **Controller**—A selected controller that is associated and regularly exchanges location information with a mobility services engine. 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 mobility services engine can be synchronized with Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports.
- The mobility services engine can also be synchronized with the following Catalyst 4000 series 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](#)” section on page 3-5.
- Third Party Elements—When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.
- Service Advertisements—MSAP provides service advertisements on mobile devices. This shows the service advertisement that is synchronized with the MSE.

Prerequisites for Synchronizing the Mobility Services Engine

- Be sure to verify software compatibility between the controller, 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 mobility services engine, Prime Infrastructure, and the controller is in Coordinated Universal Time (UTC). Configuring NTP on each system provides devices with UTC time. The mobility services engine 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 mobility services engine. However, the timezone for MSE should still be set to UTC. This is because wIPS alarms require that the MSE time 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 Elements or Marking Them as Third-Party Elements

To delete 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 Controllers with a Mobility Services Engine

This section describes how to synchronize a controller, assign an MSE to any wireless controller and also to unassign a network design, controller, wired switch, or event group from a mobility services engine.

Synchronizing a Controller, Catalyst Switch, or Event Group

To synchronize network designs, a controller, 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 mobility services engine, 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 mobility services engine by selecting the corresponding **Name** check box.



Note Through Release 6.0, you can assign only up to a campus level to a mobility services engine. 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 mobility services engine to which the maps are to be synchronized.

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

- **Save**—Saves the mobility services engine assignment. The following message appears in the Messages column of the Network Designs page with a yellow arrow icon:
“To be assigned - Please synchronize”.
- **Cancel**—Discards the changes to the mobility services engine assignment and returns to the Network Designs page.

You can also click **Reset** to undo the mobility services engine assignments.



Note A network design may include a floor in a campus or a large campus with several buildings, each monitored by a different mobility services engine. Because of this, you may need to assign a single network design to multiple mobility services engines.



Note Network design assignments also automatically picks up the corresponding controller for synchronization.

- Step 8** Click **Synchronize** to update the mobility services engine(s) database(s).
When items are synchronized, a green two-arrow icon appears in the Sync. Status column for each synchronized entry.
You can use the same procedure to assign wired switches or event groups to a mobility services engine. To assign a controller to a mobility services engine, see [“Synchronizing Controllers with a Mobility Services Engine” section on page 3-3](#) for more information.

Assigning an MSE to the Controller

To assign a mobility services engine with any wireless controller 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 controllers to be assigned to the mobility services engine by selecting the corresponding **Name** check box.
- Step 4** Click **Change MSE Assignment**.
- Step 5** Choose the mobility services engine to which the controllers must be synchronized.
- Step 6** Click either of the following in the Choose MSEs dialog box:
- **Save**—Saves the mobility services engine assignment. The following message appears in the Messages column of the Controllers page with a yellow arrow icon:
“To be assigned - Please synchronize”.
 - **Cancel**—Discards the changes to mobility services engine assignment and returns to the Controllers page.
- You can also click **Reset** to undo the mobility services engine assignments.
- Step 7** Click **Synchronize** to complete the synchronization process.
- Step 8** Verify that the mobility services engine is communicating with each of the controllers for only the chosen service. This can be done by clicking the NMSP status link in the status page.



Note After Synchronizing a controller, verify that the timezone is set on the associated controller.

**Note**

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

You can use the same procedure to assign Catalyst switches or event groups to a mobility services engine.

**Note**

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

Unassigning a Network Design, Controller, Wired Switch, or Event Group from the 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** Unselect the mobility services engine if you do not want the elements to be associated with that mobility services engine by selecting either the **CAS** or **wIPS** check box.
- Step 5** Click **Save** to save the assignment changes.
- Step 6** Click **Synchronize**.
The Sync Status column appears blank.

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 mobility services engine databases is triggered periodically and any related alarms are cleared.

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

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

This section contains the following topics:

- [Configuring Automatic Database Synchronization, page 3-6](#)
- [Smart Controller Assignment and Selection Scenarios, page 3-7](#)
- [Out-of-Sync Alarms, page 3-7](#)

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.
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 mobility services engine. 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 mobility services engine.



Note When a mobility services engine is added to an Prime Infrastructure, the data in the Prime Infrastructure is always treated as the primary copy that is synchronized with the mobility services engine. All synchronized network designs, controllers, event groups and wired switches that are present in the mobility services engine and not in the Prime Infrastructure are removed automatically from mobility services engine.

- 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 **Submit**.
-

For Smart controller assignment and selection scenarios, see [“Smart Controller Assignment and Selection Scenarios”](#) section on page 3-7.

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 mobility services engine for the CAS service.

Scenario 3

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

Scenario 4

If all access points placed on a floor that is synchronized to the MSE are deleted, then that controller is automatically removed from the mobility services engine 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 controllers exist in the mobility services engine database but not in the Prime Infrastructure
- Elements are not assigned to any mobility services engine (the auto-sync policy does not apply)

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

- The mobility services engine is deleted



Note When you delete a mobility services engine, the out-of-sync alarms for that system are also deleted. In addition, if you delete the last available mobility services engine, the 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 Mobility Services Engine Synchronization Status

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.

This section contains the following topics:

- [Viewing Mobility Services Engine Synchronization Status, page 3-8](#)
- [Viewing Synchronization History, page 3-8](#)

Viewing Mobility Services Engine Synchronization Status

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, Event Groups, 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 > Site 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.

[Table 3-1](#) describes the table column headings that appear in the Synchronization History page.

Table 3-1 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 element that was synchronized.
Type	The type of the element that was synchronized.
Sync Operation	The sync operation that was performed. It can be an Update, Add, or Delete.
Generated By	The method of synchronization. It can be Manual or Automatic.

Table 3-1 Synchronization History Page

Text Boxes	Description
Status	The status of the synchronization. It can be either Success or Failed.
Message	Any additional message about the synchronization.

Click the column headings to sort the entries.



CHAPTER 4

Configuring High Availability

This chapter describes how to configure high availability on the MSE. The mobility services engine is a platform for hosting multiple mobility applications. Every active MSE is backed up by another inactive instance. The active MSE is called the primary MSE and the inactive MSE is called the secondary MSE.

The main component of high availability system is the health monitor. The health monitor configures, manages, and monitors the high availability setup. Heartbeat is maintained between the primary and secondary MSE. Health monitor is responsible for setting up the database, file replication, and monitoring the application. When the primary MSE fails and the secondary MSE takes over, the virtual address of the primary MSE is switched transparently.



Note

The Mobility Services Engines, Synchronize Services, Synchronization History, High Availability, Context Aware Notifications, and MSAP pages on the Services tab are available only in the virtual domain inRelease 7.3.

This chapter contains the following sections:

- [Overview to the High Availability Architecture, page 4-1](#)
- [Pairing Matrix, page 4-2](#)
- [Guidelines and Limitations for High Availability, page 4-2](#)
- [Failover Scenario for High Availability, page 4-2](#)
- [Failback, page 4-3](#)
- [HA Licensing, page 4-3](#)
- [Configuring High Availability on the MSE, page 4-3](#)
- [Viewing Configured Parameters for High Availability, page 4-6](#)
- [Viewing High Availability Status, page 4-7](#)

Overview to the High Availability Architecture

This section provides an overview of the high availability architecture:

- Every active primary MSE is backed up by another inactive instance. The purpose of the secondary MSE is to monitor the availability and state of the primary MSE. The secondary MSE becomes active only after the failover procedure is initiated.
- The failover procedure can be manual or automatic.

- One secondary MSE can support two primary MSEs.
- There is one software and database instance for each registered primary MSE.

Pairing Matrix

Table 4-1 lists the server type pairing matrix information.

Table 4-1 Pairing Matrix

Primary Server Type	Secondary Server Type							
		3310	3350	3355	VA-2	VA-3	VA-4	VA-5
3310	Y	Y	Y	N	N	N	N	
3350	N	Y	Y	N	N	N	N	
3355	N	Y	Y	N	N	N	N	
VA-2	N	N	N	Y	Y	Y	Y	
VA-3	N	N	N	N	Y	Y	Y	
VA-4	N	N	N	N	N	Y	Y	
VA-5	N	N	N	N	N	N	Y	

Guidelines and Limitations for High Availability

- Both the health monitor IP and virtual IP should be accessible from the Cisco Prime Infrastructure.
- The health monitor IP and virtual IP should always be different. The health monitor and virtual interface can be on the same interface or different interfaces.
- You can use either manual or automatic failover. Failover should be considered temporary. The failed MSE should be restored to normal as soon as possible, and failback will be reinitiated. The longer it takes to restore the failed MSE, the longer the other MSEs sharing the secondary MSE must run without failover support.
- You can use either manual or automatic failback.
- Both the primary and secondary MSE should be running the same software version.
- High availability over WAN is not supported.
- High availability over LAN is supported only when both the primary and secondary MSE are in the same subnet.
- The ports over which the primary and secondary MSEs communicate must be open (not blocked with network firewalls, application firewalls, gateways, and so on).

Failover Scenario for High Availability

When a primary MSE failure is detected, the following events take place:

**Note**

One secondary MSE can back up multiple primary MSEs.

- The primary MSE is confirmed as non-functioning (hardware fail, network fail, and so on) by the health monitor on the secondary MSE.
- If automatic failover has been enabled, the secondary MSE is started immediately and uses the corresponding database of the primary MSE. If automatic failover is disabled, an e-mail is sent to the administrator asking if they want to manually start failover.
- When the manual failover is configured, an e-mail is sent only if the e-mail is configured for MSE alarms. When manual failover is configured and not invoked, there is no need for failback.
- Failback is invoked and the primary MSE assumes all the operations.
- The result of the failover operation is indicated as an event in the Health Monitor UI, and a critical alarm is sent to the administrator.

Failback

When the primary MSE is restored to its normal state if the secondary MSE is already failing over for the primary, then failback can be invoked.

Failback can occur only if the secondary MSE is in one of the following states for the primary instance:

- The secondary MSE is actually failing over for the primary MSE.
- If manual failover is configured but the administrator did not invoke it.
- The primary MSE failed but the secondary MSE cannot take over because it has encountered errors or it is failing over another primary MSE.
- Failback can occur only if the administrator starts up the failed primary MSE.

HA Licensing

A separate license is not required to set up an MSE HA system. A virtual appliance secondary does not need an activation license.

Configuring High Availability on the MSE

Configuring high availability on the MSE involves the following two steps:

- During the installation of the MSE software, you must perform certain configurations using the command-line client.
- Pair up the primary and secondary MSE from the Prime Infrastructure UI.

**Note**

If you do not want high availability support and if you are upgrading from an older release, you can continue to use the old IP address for the MSE. If you want to set up high availability, then you must configure the health monitor IP address. The health monitor then becomes a virtual IP address.



Note By default, all MSEs are configured as primary.



Note The **Services > High Availability** page is available only in the virtual domain in Release 7.3.

To configure high availability on the primary MSE, follow these steps:

- Step 1** Ensure that the network connectivity between the primary and secondary is functioning and that all the necessary ports are open.
- Step 2** Install the correct version of MSE on the primary MSE.
- Step 3** Make sure that the same MSE release version that is loaded on the other primary MSE and secondary MSE is also loaded on the new primary MSE.
- Step 4** On the intended primary MSE, enter the following command:

```
/opt/mse/setup/setup.sh
```

```
-----
Welcome to the appliance setup.
Please enter the requested information. At any prompt,
enter ^ to go back to the previous prompt. You may exit at
any time by typing <Ctrl+C>.
You will be prompted to choose whether you wish to configure a
parameter, skip it, or reset it to its initial default value.
Skipping a parameter will leave it unchanged from its current
value.
Changes made will only be applied to the system once all the
information is entered and verified.
-----
```

- Step 5** Configure the hostname:

```
Current hostname=[mse]
Configure hostname? (Y)es/(S)kip/(U)se default [Skip]:
```

The hostname should be a unique name that can identify the device on the network. The hostname should start with a letter, end with a letter or number, and contain only letters, numbers, and dashes.

- Step 6** Configure the domain name:

Enter a domain name for the network domain to which the device belongs. The domain name should start with a letter, and it should end with a valid domain name suffix such as *.com*. It must contain only letters, numbers, dashes, and dots.

```
Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]:
```

- Step 7** Configure the HA role:

```
Current role=[Primary]
Configure High Availability? (Y)es/(S)kip/(U)se default [Skip]:
High availability role for this MSE (Primary/Secondary):
Select role [1 for Primary, 2 for Secondary] [1]: 1
Health monitor interface holds physical IP address of this MSE server.
This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to
communicate among themselves
Select Health Monitor Interface [eth0/eth1] [eth0]:eth0
```

```

-----
Direct connect configuration facilitates use of a direct cable connection between the
primary and secondary MSE servers.
This can help reduce latencies in heartbeat response times, data replication and failure
detection times.
Please choose a network interface that you wish to use for direct connect. You should
appropriately configure the respective interfaces.
\"none\" implies you do not wish to use direct connect configuration.
-----

```

Step 8 Configure Ethernet interface parameters:

```

Select direct connect interface [eth0/eth1/none] [none]: eth0
Enter a Virtual IP address for first this primary MSE server:
Enter Virtual IP address [172.31.255.255]:
Enter the network mask for IP address 172.31.255.255.
Enter network mask [255.255.255.0]:
Current IP address=[172.31.255.255]
Current eth0 netmask=[255.255.255.0]
Current gateway address=[172.31.255.256]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:

```

Step 9 When prompted for “eth1” interface parameters, enter Skip to proceed to the next step. A second NIC is not required for operation:

```

Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:

```

Follow [Step 10](#) through [Step 13](#) to configure the secondary MSE.

Step 10 Configure the hostname for the secondary MSE:

```

Current hostname=[]
Configure hostname? (Y)es/(S)kip/(U)se default [Skip]:

```

Step 11 Configure the domain name:

```

Current domain=
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]:

```

Step 12 Configure the HA role:

```

Current role=[Primary]
Configure High Availability? (Y)es/(S)kip/(U)se default [Skip]:
High availability role for this MSE (Primary/Secondary)
Select role [1 for Primary, 2 for Secondary] [1]: 2
Health monitor interface holds physical IP address of this MSE server.
This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to
communicate among themselves
Select Health Monitor Interface [eth0/eth1] [eth0]:[eth0/eth1]
-----
Direct connect configuration facilitates use of a direct cable connection between the
primary and secondary MSE servers.
This can help reduce latencies in heartbeat response times, data replication and failure
detection times.
Please choose a network interface that you wish to use for direct connect. You should
appropriately configure the respective interfaces.
\"none\" implies you do not wish to use direct connect configuration.
-----

```

Step 13 Configure Ethernet interface parameters:

```

Select direct connect interface [eth0/eth1/none] [none]: eth1

```

```

Enter a Virtual IP address for first this primary MSE server
Enter Virtual IP address [172.19.35.61]:
Enter the network mask for IP address 172.19.35.61:
Enter network mask [255.255.254.0]:
Current IP address=[172.19.35.127]
Current eth0 netmask=[255.255.254.0]
Current gateway address=[172.19.34.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:

```

- Step 14** Once you have configured both the primary MSE and secondary MSE, the Prime Infrastructure UI should be used to set up a pairing between the primary and secondary MSE.
- Step 15** Once the primary MSE is added successfully, choose **Services > High Availability** or click the primary MSE device in the **Services > Mobility Services Engine** page, and choose **HA Configuration > Service High Availability** from the left sidebar menu.
- The HA Configuration page appears.
- Step 16** Enter the secondary device name with which you want to pair the primary MSE.
- Step 17** Enter the secondary IP address which is the health monitor IP address of the secondary MSE.
- Step 18** Enter the secondary password. This is the Prime Infrastructure communication password configured on the MSE.
- Step 19** Specify the failover type. You can choose either **Manual** or **Automatic** from the Failover Type drop-down list. After 10 seconds, the system fails over. The secondary server waits for a maximum of 10 seconds for the next heartbeat from the primary server. If it does not get the heartbeat in 10 seconds, it declares a failure.
- Step 20** Specify the failback type by choosing either **Manual** or **Automatic** from the Failback Type drop-down list.
- Step 21** Specify the Long Failover Wait in seconds.
- After 10 seconds, the system fails over. The maximum failover wait is 2 seconds.
- Step 22** Click **Save**.
- The pairing and the synchronization happens automatically.
- Step 23** To check whether the heartbeat is received from the primary MSE or not, choose **Services > Mobility Services Engine**, and click **Device Name** to view the configured parameters.
- Step 24** Choose **HA Configuration > Service High Availability** from the left sidebar menu.
- Check whether the heartbeat is received from the primary MSE or not.

Viewing Configured Parameters for High Availability

To view the configured parameters for high availability, follow these steps:

- Step 1** Choose **Services > High Availability**.
- Step 2** Click **Device Name** to view its configured fields.
- The HA configuration page appears.
- Step 3** Choose **Services High Availability > HA Configuration** from the left sidebar menu. The HA Configuration page shows the following information:

- Primary Health Monitor IP
 - Secondary Device Name
 - Secondary IP Address
 - Secondary Password
 - Failover Type
 - Failback Type
 - Long Failover Wait
-

Viewing High Availability Status

To view the high availability status, follow these steps:

-
- Step 1** Choose **Services > High Availability**.
- Step 2** Click **Device Name** to view the desired status.
The HA Configuration page appears.
- Step 3** Choose **Services High Availability > HA Status** from the left sidebar menu. The HA Configuration page shows the following information:
- Current high Availability Status
 - Status—Shows whether the primary and secondary MSE instances are correctly synchronized or not.
 - Heartbeats—Shows whether the heartbeat is received from the primary MSE or not.
 - Data Replication—Shows whether the data replication between the primary and secondary databases is happening or not.
 - Mean Heartbeat Response Time—Shows the mean heartbeat response time between the primary and secondary MSE instance.
 - Event Log—Shows all the events generated by the MSE. The last 20 events can be viewed.
-



CHAPTER 5

MSE Delivery Modes

The Cisco MSE comes preinstalled on a physical appliance with various performance characters. The MSE is delivered in two modes, the physical appliance and the virtual appliance.

This chapter contains the following sections:

- [Physical Appliance, page 5-1](#)
- [Virtual Appliance, page 5-1](#)

Physical Appliance

When the MSE is located on the physical appliance, you can use the standard license center UI to add new licenses. When the MSE is located on the physical appliance, the license installation process is based on Cisco UDI (Unique Device Identifier). Choose **Administration > License Center** on the Cisco Prime Infrastructure UI to add the license.



Note

Virtual appliance licenses are not allowed on physical appliances.

Virtual Appliance

MSE is also offered as a virtual appliance, to support lower-level, high, and very high end deployments. When the MSE is located on the virtual appliance, the license is validated against VUDI (Virtual Unique Device Identifier) instead of UDI.



Note

MSE is available as a virtual appliance for Release 7.2 and later. The virtual appliance must be activated first before installing any other service licenses.

The MSE virtual appliance software is distributed as an Open Virtualization Archive (OVA) file. You can install the MSE virtual appliance using any of the methods for deploying an OVF supported by the VMware environment. Before starting, make sure that the MSE virtual appliance distribution archive is in a location that is accessible to the computer on which you are running vSphere Client.

For a virtual appliance, you must have an activation license. Without an activation license, the MSE starts in evaluation mode. Even if service licenses are present on the host, it rejects them if the activation license is not installed.

**Note**

See the VMware vSphere 4.0 documentation for more information about setting up your VMware environment.

You can add and delete a virtual appliance license either using the **Services > Mobility Services Engine > Add Mobility Services Engine** page when you are installing MSE for the first time, or you can use **Administration > License Center** page to add or delete a license.

See the “[Adding a Mobility Services Engine to the Prime Infrastructure](#)” section on page 2-4 and the “[Deleting a Mobility Services Engine from the Prime Infrastructure](#)” section on page 2-7 for more information on adding a license and deleting a license using the mobility services engine wizard.

This section contains the following topics:

- [Operating Systems Requirements, page 5-2](#)
- [Client Requirements, page 5-2](#)
- [Reinstalling the MSE on a Physical Appliance, page 5-3](#)
- [Deploying the MSE Virtual Appliance, page 5-4](#)
- [Adding a License File to the MSE Using the License Center, page 5-8](#)
- [Viewing the MSE License Information Using the License Center, page 5-9](#)
- [Removing a License File Using the License Center, page 5-9](#)

Operating Systems Requirements

The following operating systems are supported:

- Red Hat Linux Enterprise server 5.4 64-bit operating system installations are supported.
- Red Hat Linux version support on VMware ESX/ESXi Version 4.1 and later with either local storage or SAN over fiber channel.

**Note**

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

Client Requirements

The MSE user interface requires Microsoft Internet Explorer 7.0 or later with the Google Chrome plugin or Mozilla Firefox 3.6 or later releases.

**Note**

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

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

Prerequisites for Setting Up an MSE Virtual Appliance on a Server

Before setting up an MSE virtual appliance, ensure that you have completed the following:

- Make sure that your computer has at least 500 GB of hard disk space and fast SAS drives with enhanced RAID controllers.
- Use VM ESXi 4.1 or later.
- Insert the ESXi 4.1 or later DVD and boot from the drive. Install ESXi. If there are multiple drives, install in the drive that is configured as the boot drive. If you select the wrong drive for install, you can reformat using a Fedora Live CD and select the other drive when you install ESXi again.
- Default username and password for ESX/i are root and blank, just leave blank and hit enter (no password).
- Configure the IP address and make sure to select the correct Network Adapter (select the ones that are enabled and active, you might have multiple if your host is connected to multiple networks).
- (If you are using UCS box) - You can also set the same IP address during CIMC setup (press F8 during boot up). Also change the default password.
- Once ESXi is setup, you can use a Win XP/7 machine and connect to the ESXi host through vSphere client using the above configured IP address and login credentials.
- Refer to following articles to setup the datastores on ESXi:
 - <http://pubs.vmware.com/vsphere-esxi-4-1-embedded/wwhelp/wwhimpl/js/html/wwhelp.htm>

Virtual Appliance Sizing

See [Table 5-1](#) for information on virtual appliance sizing.

Table 5-1 Virtual Appliance Sizing

Primary MSE Virtual Appliance Level	Resources		Supported License (Individually)	
	Total Memory	CPU	CAS License	wIPS License
Level1	3.5G	1	100	20
Level2	6G	2	2000	2000
Level3	11G	8	18000	5000
Level4	20G	16	50000	10000

Reinstalling the MSE on a Physical Appliance

You must have root privileges to install the MSE on a physical appliance. To reinstall the MSE on a physical appliance, follow these steps:

-
- Step 1** Insert the provided MSE software image DVD. The system boots up and a console appears.
- Step 2** Select option 1 to reinstall the MSE software image. The system reboots and the configure appliance screen appears.

- Step 3** Enter the initial setup parameters and the system reboots again. Remove the DVD and follow the provided steps to start the MSE server.
-

Deploying the MSE Virtual Appliance

This section describes how to deploy the MSE virtual appliance on an ESXi host using the vSphere Client using the Deploy OVF wizard or from the command line. This section contains the following topics:

- [Deploying the MSE Virtual Appliance from the VMware vSphere Client, page 5-4](#)
- [Configuring the Basic Settings to Start the MSE Virtual Appliance VM, page 5-7](#)
- [Deploying the MSE Virtual Appliance Using the Command-Line Client, page 5-8](#)

Deploying the MSE Virtual Appliance from the VMware vSphere Client

The MSE virtual appliance is distributed as an OVA file that can be deployed on an ESXi using the vSphere Client. An OVA is a collection of items in a single archive. In the vSphere Client, you can deploy the OVA wizard to create a virtual machine running the MSE virtual appliance application as described in this section.



Note While the following procedure provides general guidelines for how to deploy the MSE virtual appliance, the exact steps that you must perform may vary depending on the characteristics of your VMware environment and setup.

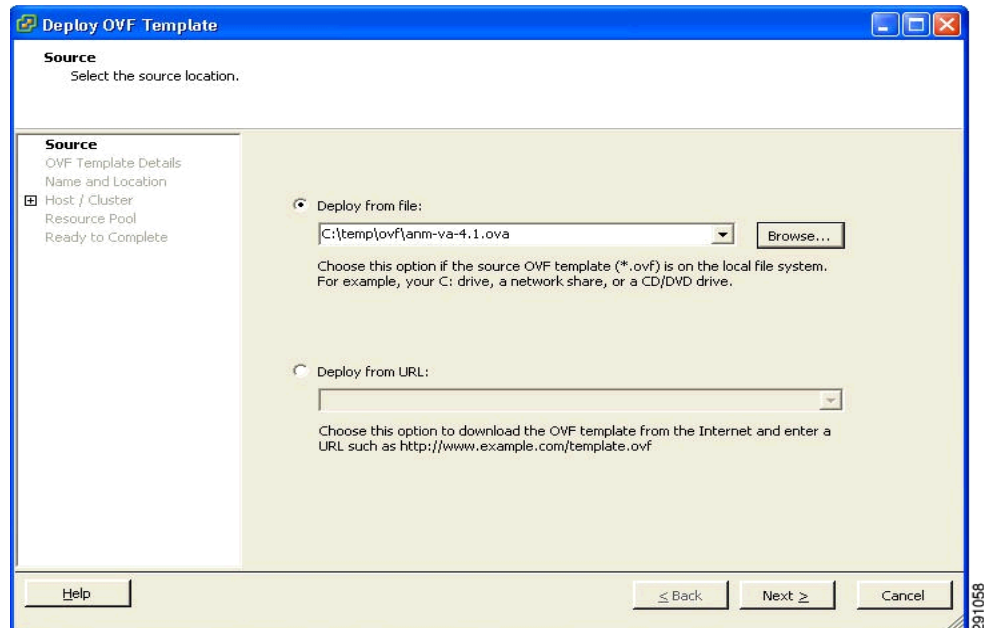


Note Deploying virtual appliance takes at least 500 GB of available disk space on the ESXi host database. We recommend that the datastore on the host have a block size of at least 4 MB or more for ESXi 4.1 or earlier, else the deployment may fail. No such restriction is placed on the datastores on ESXi 5.0 and later.

To deploy the MSE virtual appliance, follow these steps:

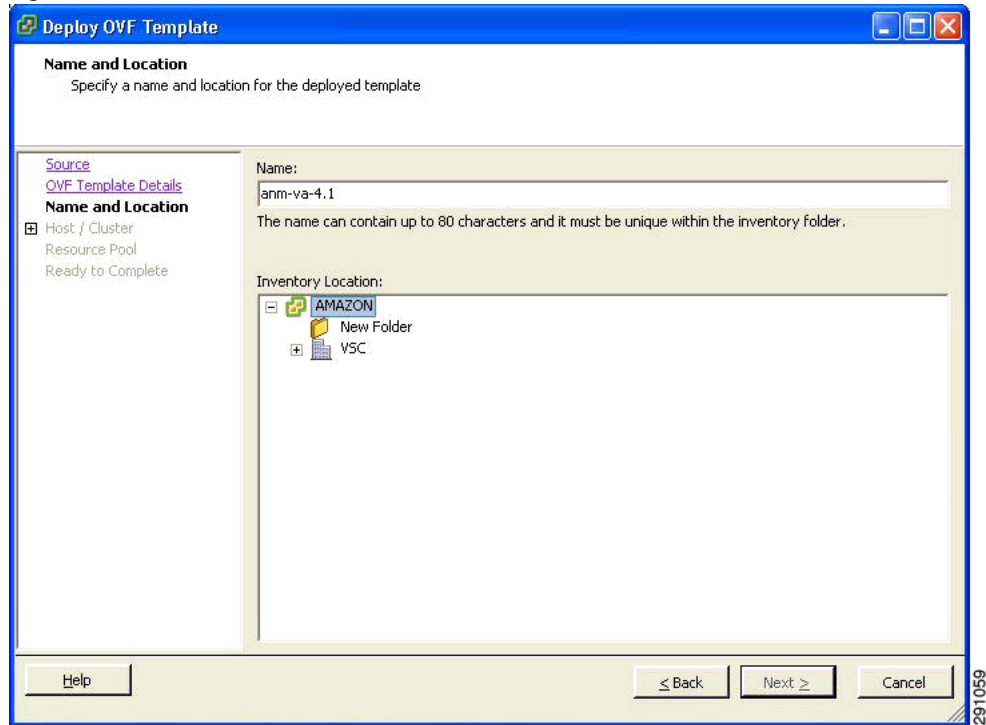
- Step 1** From the VMware vSphere Client main menu, choose **File > Deploy OVF Template**. The OVF Template Source window appears (see [Figure 5-1](#)).

Figure 5-1 Deploy OVF Template Window



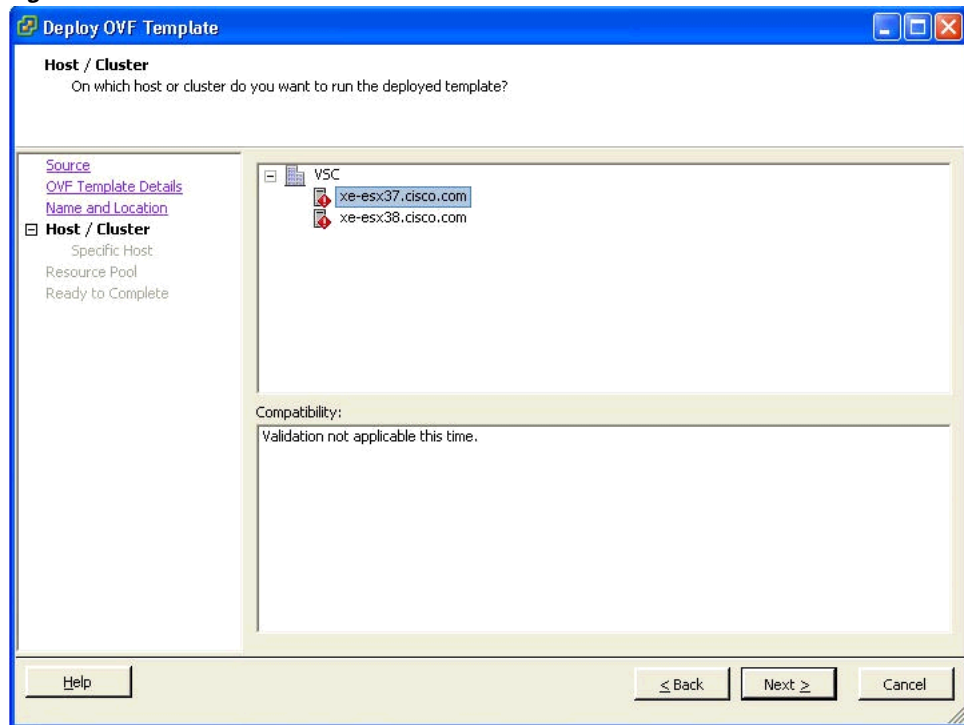
- Step 2** Select the **Deploy From File** radio button and choose the OVA file that contains the MSE virtual appliance distribution from the drop-down list.
- Step 3** Click **Next**. The OVF Template Details window appears. VMware ESX/ESXi reads the OVA attributes. The details include the product you are installing, the size of the OVA file (download size), and the amount of disk space that must be available for the virtual machine.
- Step 4** Verify the OVF Template details and click **Next**. The Name and Location window appears (see [Figure 5-2](#)).

Figure 5-2 Name and Location Window



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

Figure 5-3 Host/Cluster Window



- Step 6** Choose the destination host or HA cluster on which you want to deploy the MSE VM, and click **Next**. The Resource Pool window appears.
- Step 7** If you have more than one resource pool in your target host environment, choose the resource pool to use for the deployment, and click **Next**. The Ready to Complete window appears.
- Step 8** Review the settings shown for your deployment and, if needed, click **Back** to modify any of the settings shown.
- Step 9** Click **Finish** to complete the deployment. A message notifies you when the installation completes and you can see the MSE virtual appliance in your inventory.
- Step 10** Click **Close** to close the Deployment Completed Successfully dialog box.

Configuring the Basic Settings to Start the MSE Virtual Appliance VM

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

To start the MSE setup, follow these steps:

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

- Step 2** On the Getting Started tab, click the **Power** on the virtual machine link in Basic Tasks. The Recent Tasks window at the bottom of the vSphere Client pane indicates the status of the task associated with powering on the virtual machine. After the virtual machine successfully starts, the status column for the task shows Completed.
- Step 3** Click the **Console** tab, within the console pane to make the console prompt active for keyboard input.
- Step 4** Use the MSE setup wizard to complete the setup.
-

Deploying the MSE Virtual Appliance Using the Command-Line Client

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

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

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

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

Adding a Virtual Appliance License to the Prime Infrastructure

You can add a virtual appliance license to the Prime Infrastructure using the following two options:

- Using the Add Mobility Service Engine page when you are installing MSE for the first time. See [“Adding a Mobility Services Engine to the Prime Infrastructure” section on page 2-4](#) for more information.
- Using the License Center page. See [“Adding a License File to the MSE Using the License Center” section on page 5-8](#) for more information.

Adding a License File to the MSE Using the License Center

To add a license, follow these steps:

-
- Step 1** Install the MSE virtual appliance.
- Step 2** Add the MSE to the Prime Infrastructure.
- Step 3** Choose **Administration > License Center** in the Prime Infrastructure UI to access the License Center page.
- Step 4** Choose **Files > MSE Files** from the left sidebar menu.
- Step 5** Click **Add** to add a license.
The Add A License File menu appears.
- Step 6** Select the MSE and browse to the activation license file.
- Step 7** Click **Submit**.

Once you submit, the license is activated and license information appears in the License Center page.

Viewing the MSE License Information Using the License Center

The license center allows you to manage the Prime Infrastructure, Wireless LAN Controllers, and MSE licenses. To view the license information, follow these steps:

- Step 1** Choose **Administration > License Center** to access the License Center page.
- Step 2** Choose **Summary > MSE** from the left sidebar menu to view the MSE summary page.

[Table 5-2](#) lists the MSE Summary page fields.

Table 5-2 MSE Summary Page

Field	Description
MSE Name	Provides a link to the MSE license file list page.
Service	Service type can be CAS or wIPS.
Platform Limit	Platform limit.
Type	Specifies the type of MSE.
Installed Limit	Shows the total number of client elements licensed across MSEs.
License Type	The three different types of licenses: permanent, evaluation, and extension.
Count	The number of CAS or wIPS elements currently licensed across MSEs.
Unlicensed Count	Shows the number of client elements that are not licensed.
%Used	The percentage of CAS or wIPS elements licensed across MSEs.

Removing a License File Using the License Center

To remove a license, follow these steps:

- Step 1** Install the MSE virtual appliance.
- Step 2** Add the MSE to the Prime Infrastructure using the wizard.
- Step 3** Choose **Administration > License Center** to access the License Center page.
- Step 4** Choose **Files > MSE Files** from the left sidebar menu.
- Step 5** Choose an MSE license file that you want to remove by selecting the **MSE License File** radio button, and click **Remove**.

Step 6 Click **OK** to confirm the deletion.



CHAPTER 6

Configuring and Viewing System Properties

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

This chapter contains the following sections:

- [Licensing Requirement, page 6-1](#)
- [Editing General Properties and Viewing Performance, page 6-1](#)
- [Viewing Active Sessions on a System, page 6-5](#)
- [Adding and Deleting Trap Destinations, page 6-6](#)
- [Viewing and Configuring Advanced Parameters, page 6-7](#)
- [Initiating Advanced Parameters, page 6-8](#)

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. Licenses are usage-based (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 mobility services engine for synchronization. See the [“Editing General Properties” section on page 6-2](#) for more information.



Note

Use the general properties to modify the username and password that you defined during initial setup of the mobility services engine.

Performance—You can use the Prime Infrastructure to view CPU and memory usage for a given mobility services engine. See the [“Viewing Performance Information” section on page 6-4](#) for more information.

This section contains the following topics:

- [Editing General Properties, page 6-2](#)
- [Viewing Performance Information, page 6-4](#)

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 mobility services engine 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. [Table 6-1](#) lists the General Properties page fields.

Table 6-1 General Tab

Field	Configuration Options
Device Name	User-assigned name for the mobility services engine.
Device Type	Indicates the type of mobility services engine (for example, Cisco 3310 Mobility Services Engine). Indicates whether the device is a virtual appliance or not.
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 mobility services engine.
Contact Name	Enter a contact name for the mobility services engine.
Username	Enter the login username for the Prime Infrastructure server that manages the mobility services engine. 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 mobility services engine. This replaces any previously defined password including any set during initial setup.
HTTP	Select the Enable check box to enable HTTP. By default, HTTPS is enabled. Note HTTP is primarily enabled to allow third-party applications to communicate with the mobility services engine. Note Prime Infrastructure always communicates through HTTPS.
Legacy Port	Enter the mobility services port number that supports HTTPS communication. The Legacy HTTPS option must also be enabled.

Table 6-1 General Tab (continued)

Field	Configuration Options
Legacy HTTPS	This does not apply to mobility services engines. It applies only to location appliances.
Delete synchronized service assignments and enable synchronization	Select this check box if you want to permanently remove all service assignments from the mobility services engine. This option is available only if the delete synchronized service assignments check box was unselected while adding a mobility services engine.
Mobility Services	<p>To enable a service on the mobility services engine, select the check box next to the service. The services include Context Aware and wIPS.</p> <p>You can choose CAS to track clients, rogues, interferers, wired clients, and tags.</p> <p>Choose either of the following engines to track tags:</p> <ul style="list-style-type: none"> • Cisco Tag Engine or • Partner Tag Engine <p>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.</p> <p>Note CAS and wIPS can operate on a mobility services engine at the same time.</p> <p>Click the here link to see the number of devices that can be assigned for the current system.</p> <p>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.</p> <p>Note For more information on purchasing and installing licenses, see the following URL:</p> <p>http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/d_ata_sheet_c07-473865.html</p>

**Note**

The following tcp ports are in use on the MSE in Release 6.0: tcp 22: MSE SSH port, tcp 80: MSE HTTP port, tcp 443: MSE HTTPS port, tcp 1411: AeroScout, tcp 1999: AeroScout internal port, tcp 4096: AeroScout notifications port, tcp 5900X: AeroScout (X can vary from 1 to 10), and tcp 8001: Legacy port. Used for location APIs.

**Note**

The following udp ports are in use on the MSE in Release 6.0: udp 123: NTPD port (open after NTP configuration), udp 162: AeroScout SNMP, udp/tcp 4000X: AeroScout proxy (X can vary from 1 to 5), udp 12091: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints), udp 12092: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints), udp 32768: Location internal port, udp 32769: AeroScout internal port, and udp 37008: AeroScout internal port.



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.

Figure 6-1 License Summary for Selected Mobility Services Engine

The screenshot shows the Cisco Prime Network Control System interface. The breadcrumb navigation is Administration > License Center > Summary > MSE. A note states: "Permanent licenses include installed license counts and in-built license counts." Below this is a table with the following data:

MSE Name (UDI)	Service	Platform Limit	Type	Installed Limit	License Type	Count	Unlicensed Count	% Used
sal-mse (AIR-MSE-9310-K9-VD1:Not Specified)								
	CAS	2000	CAS Elements	2000	Permanant	923	0	46%
	wIPS	2000	wIPS Monitor Mode AEs	10	Evaluation (60 days left)	0	0	0%
			wIPS Local Mode APs	10	Evaluation (60 days left)	0	0	0%
	MSAP	2000	Service Advertisement Clks	1000	Evaluation (60 days left)	0	0	0%

At the bottom right of the table area, it says "Entries 1 - 1 of 1".

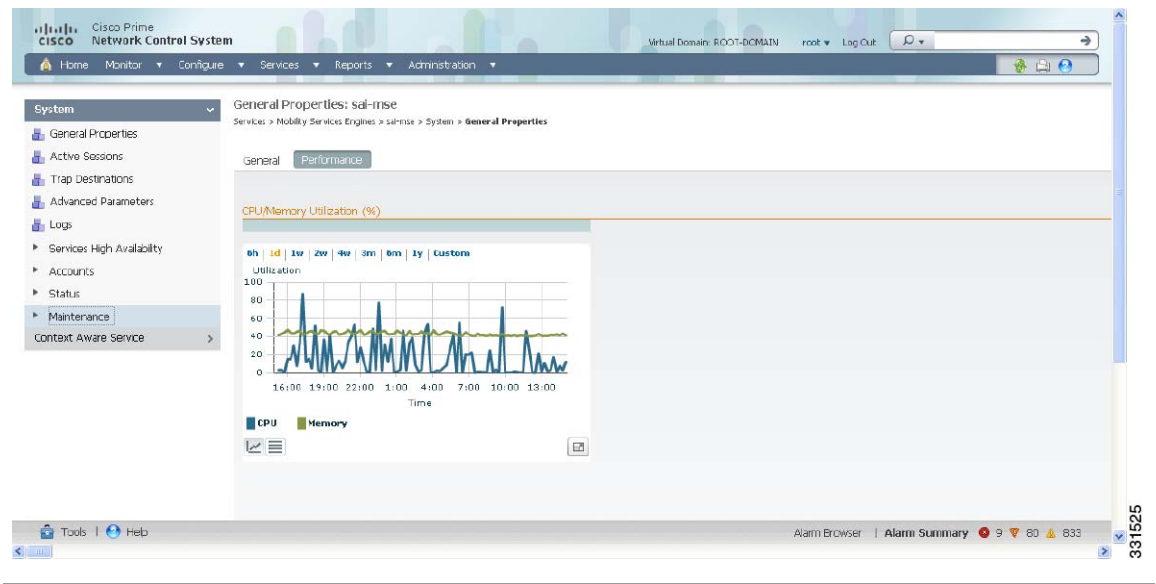
Step 4 Click **Save** to update the Prime Infrastructure and mobility services engine databases.

Viewing Performance Information

To view performance details, follow these steps:

- Step 1** Choose **Services > Mobility Services** to display the Mobility Services page.
- Step 2** Click the name of the mobility services engine you want to view. Two tabs appear with the following headings: General and Performance.
- Step 3** Click the **Performance** tab (see [Figure 6-2](#)).
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.

Figure 6-2 CPU and Memory Performance



Viewing Active Sessions on a System

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

For every session, the Prime Infrastructure shows the following information:

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

To view active user sessions, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**.
 - Step 2** Click the name of the mobility services engine to view its active sessions.
 - Step 3** Choose **System > Active Sessions**.
-

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.

This section contains the following topics:

- [Adding Trap Destinations, page 6-6](#)
- [Deleting Trap Destinations, page 6-7](#)

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.

[Table 6-2](#) lists the Add Trap Destination page fields.

Table 6-2 Add Trap Destination Page Fields

Field	Description
IP Address	IP address for the trap destination.
Port No.	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	Username for the SNMP Version 3.
Security Name	Security name for the SNMP Version 3.
Auth. Type	Choose either of the following from the drop-down list: <ul style="list-style-type: none"> • HMAC-MD5 • HMAC-SHA

Table 6-2 Add Trap Destination Page Fields (continued)

Field	Description
Auth. Password	Authentication password for the SNMP Version 3.
Privacy Type	Choose one of the following from the drop-down list: <ul style="list-style-type: none"> • CBC-DES • CFB-AES-128 • CFB-AES-192 • CFB-AES-256
Privacy Password	Privacy password for the SNMP Version 3.



Note All trap destinations are identified as *other* except for 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 (see [Figure 6-3](#)) you can view general system level settings of the mobility services engine and configure monitoring parameters.

- See the “[Viewing Advanced Parameter Settings](#)” section on page 6-8 to view current system-level advanced parameters.

- See the “Initiating Advanced Commands” section on page 6-10 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** (see Figure 6-3).

Figure 6-3 Advanced Parameters Page

The screenshot shows the Cisco Prime Network Control System interface. The breadcrumb navigation is: Services > Mobility Services Engines > mse-sameer > System > Advanced Parameters. The page title is "Advanced Parameters: mse-sameer".

The left sidebar contains a navigation tree with the following items: System (selected), General Properties, Active Sessions, Trap Destinations, Advanced Parameters (selected), Logs, Services High Availability, HA Configuration, HA Status, Accounts, Status (selected), Maintenance, Backup, Restore, Downloaded Software, Context Aware Service, and Concerge Service.

The main content area is divided into several sections:

- General Information:**

Product Name	Cisco Mobility Service Engine	Product Identifier (PID)	AIR-MSE-3350-K9
Version	7.2.1.28	Version Identifier (VID)	V01
Started At	2011-Dec-05, 13:38:17 PST	Serial Number (SN)	USE80HN72C
Current Server Time	2011-Dec-11, 02:25:23 PST		
Hardware Restarts	41		
Active Sessions	1		
- Cisco LDI:** (Empty section)
- Advanced Commands:**
 - Reboot Hardware
 - Shutdown Hardware
 - Clear Database
 - Retain current service assignments in NCS
- Advanced Parameters:**
 - Number of Days to keep Events: (range: 1 - 365 days)
 - Session Timeout: minutes

Buttons for "Save" and "Cancel" are located at the bottom of the Advanced Parameters section.

The bottom status bar shows: Tools | Help | Alarm Browser | Alarm Summary | 8 | 0 | 597 | 331624

Initiating Advanced Parameters

The Advanced Parameters section 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 amount of time before a session times out.

For more information, see the “[Configuring Advanced Parameters](#)” section on page 6-9.

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

For more information, see the “[Initiating Advanced Commands](#)” section on page 6-10.

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 Restarts
 - 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 mobility services engine.
 - Version Identifier (VID)—The version number of the mobility services engine.
 - Serial Number (SN)—Serial number of the mobility services engine.
 - Advanced Commands
 - Reboot Hardware—Click to reboot the mobility services hardware. See “[Rebooting or Shutting Down a System](#)” section on page 6-10 for more information.
 - Shutdown Hardware—Click to turn off the mobility services hardware. See “[Rebooting or Shutting Down a System](#)” section on page 6-10 for more information.

- Clear Database—Click to clear the mobility services database. See “[Clearing the System Database](#)” section on page 6-10 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.

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.

This section contains the following topics:

- [Rebooting or Shutting Down a System, page 6-10](#)
- [Clearing the System Database, page 6-10](#)

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** (see [Figure 6-3](#)).
- 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 7

Managing Users and Groups

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

This chapter contains the following sections:

- [Prerequisites, page 7-1](#)
- [Guidelines and Limitations, page 7-1](#)
- [Managing User Groups, page 7-1](#)
- [Managing Users, page 7-3](#)

Prerequisites

Full access is required for Cisco Prime Infrastructure to access mobility services engines.

Guidelines and Limitations

Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with *read only* access, that user is unable to configure mobility services engine settings.

Managing User Groups

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

User groups allow you to assign different access privileges to users.

This section contains the following topics:

- [Adding User Groups, page 7-1](#)
- [Deleting User Groups, page 7-2](#)
- [Changing User Group Permissions, page 7-2](#)

Adding User Groups

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



Note The Services > Mobility Services Engine page is available only in root virtual domain.

- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the mobility services engine to which you want to add a user group.
- Step 3** Choose **System > Accounts > Groups**.
- Step 4** From the Select a command drop-down list, choose **Add Group**. Click **Go**.
- Step 5** Enter the name of the group in the Group Name text box.
- Step 6** Choose a permission level (**read**, **write**, or **full**) from the Permission drop-down list.



Note Full access is required for the Prime Infrastructure to access mobility services engines.

- Step 7** Click **Save**.
-

Deleting User Groups

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

- Step 1** Choose **Services > Mobility Services Engines**.
 - Step 2** Click the name of the mobility services engine from which you want to delete a user group.
 - Step 3** Choose **System > Accounts > Groups**.
 - Step 4** Select the check boxes of the groups that you want to delete.
 - Step 5** From the Select a command drop-down list, choose **Delete Group**, and click **Go**.
 - Step 6** Click **OK**.
-

Changing User Group Permissions



Caution Group permissions override individual user permissions. For example, if you give user a full access and add that user to a group with only read access, that user is unable to configure mobility services engine settings.

To change user group permissions, follow these steps:

- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the mobility services engine you want to edit.
- Step 3** Choose **System > Accounts > Groups**.
- Step 4** Click the name of the group you want to edit.

- Step 5** From the Permission drop-down list, choose a permission level (**read, write, full**).
- Step 6** Click **Save**.
-

Managing Users

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

This section contains the following topics:

- [Adding Users, page 7-3](#)
- [Deleting Users, page 7-3](#)
- [Changing User Properties, page 7-4](#)

Adding Users



Caution

Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with only read access, that user is unable to configure mobility services engine settings.

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

- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the mobility services engine to which you want to add users.
- Step 3** Choose **System > Accounts > Users**.
- Step 4** From the Select a command drop-down list, choose **Add User**. Click **Go**.
- Step 5** Enter the username in the Username text box.
- Step 6** Enter a password in the Password text box.
- Step 7** Reenter the password in the Confirm Password text box.
- Step 8** Enter the name of the group to which the user belongs in the Group Name text box.
- Step 9** From the Permission drop-down list, choose a permission level (**read, write, or full**).



Note

Full access is required for the Prime Infrastructure to access mobility services engines.

- Step 10** Click **Save**.
-

Deleting Users

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

-
- Step 1** Choose **Services > Mobility Services Engines**.
 - Step 2** Click the name of the mobility services engine from which you want to delete a user.
 - Step 3** Choose **System > Accounts > Users**.
 - Step 4** Select the check boxes of the users that you want to delete.
 - Step 5** From the Select a command drop-down list, choose **Delete User**. Click **Go**.
 - Step 6** Click **OK**.
-

Changing User Properties

To change user properties, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**.
 - Step 2** Click the name of the mobility services engine you want to edit.
 - Step 3** Choose **System > Accounts > Users**.
 - Step 4** Click the name of the group that you want to edit.
 - Step 5** Make the required changes to the Password and Group Name text boxes.
 - Step 6** Click **Save**.
-



CHAPTER 8

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, page 8-1](#)
- [Prerequisites, page 8-1](#)
- [Information About wIPS Configuration and Profile Management, page 8-2](#)

Guidelines and Limitations

- The mobility services engine can only be configured from the Cisco Prime Infrastructure.
- If your wIPS deployment consists of a controller, access point, and MSE, you must set all the three entities to the 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*:
http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html
2. Add the mobility services engine to the Prime Infrastructure (if not already added).
3. Configure access points to operate in wIPS monitor mode. See the “[Configuring Access Points for wIPS Monitor Mode](#)” section on page 8-2.
4. Configure wIPS profiles. See the “[Configuring wIPS Profiles](#)” section on page 8-4.

Information About wIPS Configuration and Profile Management

Configuration of wIPS profiles follows a chained hierarchy starting with the 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. (See [Figure 8-1](#)).

Figure 8-1 Configuration and Update of wIPS Profiles



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

1. The configuration profile is modified on the 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, page 8-2](#)
- [Configuring Access Points for wIPS Monitor Mode, page 8-2](#)
- [Configuring wIPS Profiles, page 8-4](#)

Guidelines and Limitations

- Only Cisco Aironet 1130, 1140, 1240, 1250, 3502E and 3502I Series Access Points support wIPS monitor mode.
- The wIPS submode is supported only when the access point mode is Monitor, Local, or HREAP. But for 1130 and 1240 access points, wIPS is supported only in 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 (see [Figure 8-2](#)).

Figure 8-2 *Configure > Access Points > Radio*

<input type="checkbox"/> AP Name	Ethernet MAC	IP Address	Radio	Map Location
<input type="checkbox"/> 1240-1	00:1d:45:23:d5:a0	209.165.200.230	802.11a	Unassigned

- Step 3** In the Access Point page, unselect the **Admin Status** check box to disable the radio.

Figure 8-3 *Access Points > Radio*

[Access Point](#) > [1240-1](#) > '802.11a'

General

AP Name	1240-1
AP Base Radio MAC	00:1d:46:7e:8a:60
Admin Status	<input type="checkbox"/>
Controller	209.165.200.231
Site Config ID	0

- 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 (see [Figure 8-4](#)).

Figure 8-4 *Configure > Access Points > Access Point Detail*

General **

AP Name	<input type="text" value="1240-1"/>
Ethernet MAC	00:1d:45:23:d5:a0
Base Radio MAC	00:1d:46:7e:8a:60
Country Code	<input type="text" value="US"/>
IP Address	209.165.200.232
Admin Status	<input checked="" type="checkbox"/> Enabled
AP Static IP	<input type="checkbox"/> Enabled
AP Mode	<input type="text" value="Monitor"/>
Enhanced WIPS Engine	<input checked="" type="checkbox"/> Enabled
Monitor Mode Optimization	<input type="text" value="WIPS"/>
AP Failover Priority	<input type="text" value="Low"/>

- Step 7** Select the **Enabled** check box for the Enhanced WIPS Engine.
- Step 8** From the Monitor Mode Optimization drop-down list, choose **WIPS**.
- Step 9** Click **Save**.

- Step 10** Click **OK** when prompted to reboot the access point.
- Step 11** To reenble the access point radio, choose **Configure > Access Points**.
- Step 12** Click the appropriate access point radio (see [Figure 8-5](#)).

Figure 8-5 **Configure > Access Points > Radio**

<input type="checkbox"/> AP Name	Ethernet MAC	IP Address	Radio	Map Location
<input type="checkbox"/> 1240-1	00:1d:45:23:d5:a0	209.165.200.225	802.11a	Unassigned
<input type="checkbox"/> 1130-1	00:14:6a:1b:3b:6a	209.165.200.226	802.11a	Unassigned
<input type="checkbox"/> 1250-1	00:1b:d5:13:15:e2	209.165.200.227	802.11b/g/n	Unassigned

273130

- 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 comes 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 comes pre-setup to monitor attacks against a deployment model that utilizes an integrated solution in which both the WLAN infrastructure and wIPS access points are intermixed on the same controller.



Note

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

To configure wIPS profiles, follow these steps:

- Step 1** 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** In the Profile Parameters dialog box, choose a profile template from the Copy From drop-down list.



Note

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



Note

You cannot edit the default profile.



Note Ensure that the NMSP session is active to push the profile to the controller.

Step 4 After selecting a profile and entering a profile name, click **Save and Edit**.

Step 5 (Optional) Configure SSIDs in the SSID Group List page.

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



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

- a. Select the **MyWLAN** check box and choose **Edit Group** from the drop-down list, then click **Go**.
- b. Enter SSIDs to Monitor.
- c. 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.

- d. Click **Next**.

The Select Policy and Policy Rules summary panes appear.



Note In the Select Policy pane, you can enable or disable attacks to be detected and reported. You can also edit specific thresholds for alarms and turn on forensics.

Step 6 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).

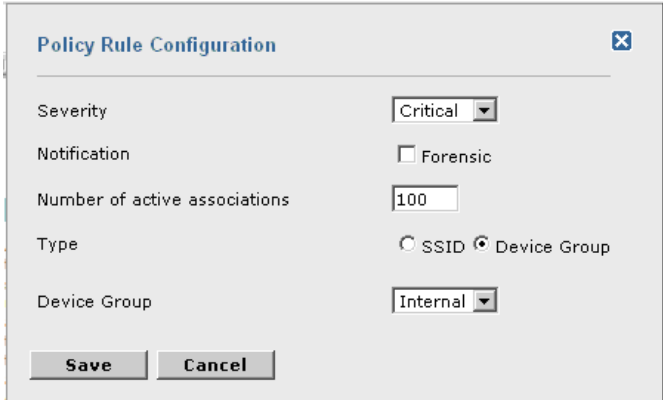
The configuration pane for that attack type appears in the right pane above the policy rule description.

Step 8 To modify a policy rule do the following:

- a. In the Policy Rules pane, select the check box next to the policy rule, and click **Edit**.

The Policy Rule Configuration dialog box appears (see [Figure 8-6](#)).

Figure 8-6 Policy Rule Configuration Dialog Box



The dialog box is titled "Policy Rule Configuration" and contains the following fields and controls:

- Severity: Critical (dropdown menu)
- Notification: Forensic
- Number of active associations: 100 (text input)
- Type: SSID Device Group
- Device Group: Internal (dropdown menu)
- Buttons: Save, Cancel

273139

- b. Choose the severity of the alarm.
- 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.
 1. If you select SSID, continue with [Step 9](#).
 2. If you select Device Group, continue with [Step 10](#).

**Note**

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

Step 9 (Optional), For overlay deployments only, to add a policy rule for an SSID, do the following:

- a. To add a policy rule, click **Add** (see [Figure 8-7](#)).

Figure 8-7 Adding a Policy Rule



The figure shows two panels: "Select Policy" and "Policy Rules".

Select Policy: A tree view showing a hierarchy of policies. "DoS: Association flood" is selected and highlighted with a red box.

Policy Rules: A table with one row: "DoS: Association flood". Below the table are buttons: "Add", "Edit", "Delete", "Move Up", and "Move Down". The "Add" button is highlighted with a red box.

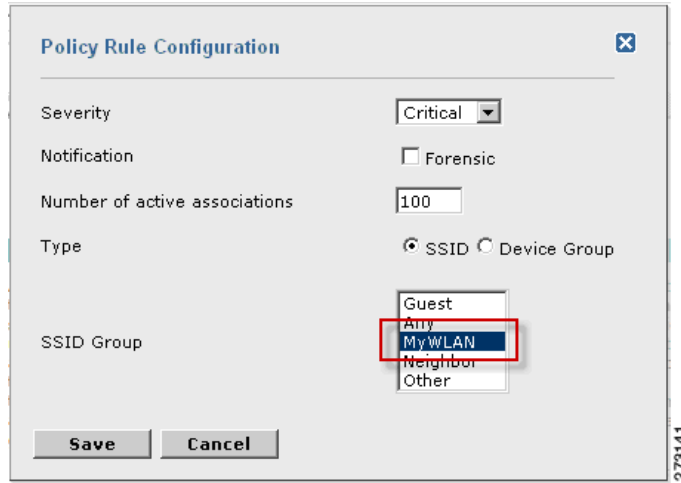
273140

- b. In the Policy Rule Configuration dialog box, choose **MyWLAN** from the SSID Group list (see [Figure 8-8](#)).

**Note**

SSID is already selected as the type.

Figure 8-8 Policy Rule Configuration Dialog Box for SSIDs



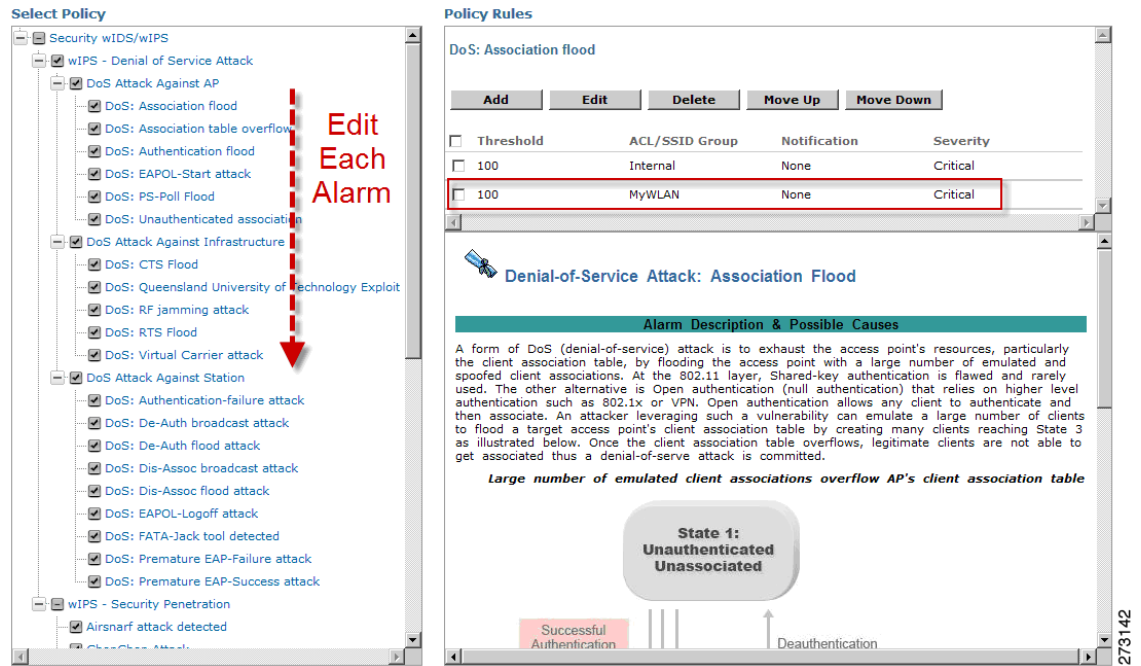
- c. Click **Save** after all changes are complete.
- d. Modify each policy rule. Continue with [Step 10](#) when all modifications are complete. (See [Figure 8-9](#)).



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 which defines the system to monitor attacks against the SSID Group created earlier.

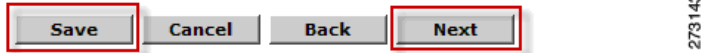
Figure 8-9 Edit Policy Rules for SSID Monitoring



- Step 10** In the Profile Configuration dialog box, click **Save** to save the Profile (SSID or Device Group). Click **Next** (see [Figure 8-10](#)).

Figure 8-10 Profile Configuration Dialog box

WIPS Profiles > Profile > 'New Profile' > Profile Configuration



- Step 11** Select the MSE/Controller combinations to apply the profile to and then click **Apply** (see [Figure 8-11](#)).

Figure 8-11 Apply Profile Dialog Box

WIPS Profiles > Profile > 'New Profile' > Apply Profile





CHAPTER 9

Monitoring the System and Services

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

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

This chapter contains the following sections:

- [Working with Alarms, page 9-1](#)
- [Working with Events, page 9-6](#)
- [Working with Logs, page 9-6](#)
- [Generating Reports, page 9-8](#)
- [Client Support on the MSE, page 9-27](#)

Working with Alarms

This section describes how to view, assign, and clear alarms and events on a mobility services engine using the Prime Infrastructure. It also describes how to define alarm notifications (all, critical, major, minor, warning) and detail how to e-mail those alarm notifications.

This section contains the following topics:

- [Guidelines and Limitations, page 9-1](#)
- [Viewing Alarms, page 9-2](#)
- [Viewing the MSE Alarm Details, page 9-2](#)
- [Assigning and Unassigning Alarms, page 9-4](#)
- [Deleting and Clearing Alarms, page 9-5](#)
- [E-mailing Alarm Notifications, page 9-5](#)

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**.



Note Alarms are displayed only in root domain. For non-root virtual domain, alarms belonging to mobility services category is not displayed in **Monitor > Alarms** page. In the Alarms Summary page, the count of mobility services alarm remains zero in non-root virtual domain.

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 to display. 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 also enter the condition in the Condition in the combo 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 State** 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](#).

Viewing the MSE Alarm Details

To view MSE alarm details, follow these steps:

Step 1 Choose **Monitor > Alarms**.

Step 2 Click an MSE in the Failure Source column to access the alarms details for a particular MSE.

Alternatively, you can choose the **Services > Services > MSE Name > System > Status > Prime Infrastructure Alarms** page and click a particular MSE item in the Failure Source column to access the alarms details for a particular MSE (see [Figure 9-1](#)).

Figure 9-1 MSE Alarm

906182

[Table 9-1](#) lists the various fields in the Alarm Detail page for an MSE.

Table 9-1 General Parameters

Field	Description
Failure Source	The MSE that generated the alarm.
Owner	Name of person to which this alarm is assigned, or blank.
Acknowledged	Shows whether or not the alarm is acknowledged by the user.
Category	The category of the alarm. The Alarm category is Mobility Services for MSEs.
Created	Month, day, year, hour, minute, second, AM or PM alarm created.
Modified	Month, day, year, hour, minute, second, AM or PM the alarm was last modified.
Generated By	This field displays the MSE.
Severity	Level of security: Critical, Major, Minor, Warning, Clear, Info, Color coded.
Previous Severity	Critical, Major, Minor, Warning, Clear, Info. Color coded.



Note

The General information may vary depending on the type of alarm. For example, some alarm details may include location and switch port tracing information.

- **Annotations**—Enter any new notes in this text box and click **Add** to update the alarm. Notes appear in the Annotations display page.
- **Messages**—Shows information about the alarm.
- **Audit Report**—Click to view config audit alarm details. This report is only available for Config Audit alarms.

Configuration audit alarms are generated when audit discrepancies are enforced on config groups.



Note If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group.

The alarms have links to the audit report where you can view a list of discrepancies for each controller.

- **Event History**—Opens the MSE Alarm Events page to view events for this alarm. When there are multiple alarm page, the page numbers appear at the top of the page with a scroll arrow on each side. Use these scroll arrows to view additional alarms.

Select a Command

The Select a command drop-down list provides access to the following functions:

- **Assign to me**—Assign the selected alarm(s) to the current user.
- **Unassign**—Unassign the selected alarm(s).
- **Delete**—Delete the selected alarm(s).
- **Clear**—Clear the selected alarm(s).



Note Once the severity is Clear, the alarm is deleted from the Prime Infrastructure after 30 days.

- **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**—Opens the All Alarms > Email Notification page to view and configure e-mail notifications.
- **Event History**—Opens the Monitor > Events page to view events for this alarm.

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

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, follow these steps:

-
- Step 1** Choose **Monitor > Alarms**.
- Step 2** From the Select a command drop-down list, choose **Email Notification**. Click **Go**. 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 the 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 event category.

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 list boxes. Click **Go**.

Step 3 If the 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.

This section contains the following topics:

- [Guidelines and Limitations, page 9-6](#)
- [Configuring Logging Options, page 9-7](#)
- [MAC Address-based Logging, page 9-8](#)
- [Downloading Log Files, page 9-8](#)



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 the 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 mobility services engine that you want to configure.
- Step 3** From the System menu, choose **Logs**. 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 [Downloading Log Files, page 9-8](#).
- 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 [“MAC Address-based Logging” section on page 9-8](#).

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 the Prime Infrastructure to download them to your system. 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 Engines**.
 - 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.
-

Generating Reports

In the Prime Infrastructure, you can generate various kinds of reports. This section explains how to generate ContextAware 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.
 - ConnectionAll 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) 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.



Note /localdisk/ftp/reports/Inventory/<ReportTitleName>_<yyyymmdd>_<HHMMSS>.csv
/localdisk/ftp/reports/Inventory/,ReportTitleName>_<yyyymmdd>_<HHMMSS>.pdf

- Monthly—The report runs on the interval indicated by the number of months you enter in the Every text box.

- Report Generation method—Choose the appropriate report generation method from the drop-down list. The possible methods are **Scheduled**, **On-demand Export**, and **On-demand Email**.

MSE Analytics

MSE Analytics reports are generated based on location history data. This section lists and describes the various MSE analytics reports that you can generate through the Prime Infrastructure Report Launch Pad.

To generate a MSE analytics report, click **New** that is next to a type to create a new report.

Click a report type to view currently saved reports. In this page, you can enable, disable, delete, or run currently saved reports.

This section describes the MSE Analytics report that you can create and contains the following topics:

- [Client Location, page 9-9](#)
- [Client Location Density, page 9-11](#)
- [Device Count by Zone, page 9-13](#)
- [Device Dwell Time by Zone, page 9-14](#)
- [Guest Location Density, page 9-16](#)
- [Location Notifications by Zone, page 9-17](#)
- [Mobile MAC Statistics, page 9-19](#)
- [Rogue AP Location Density, page 9-20](#)
- [Creating a Device Utilization Report, page 9-22](#)

Client Location

This report shows historical location history of a wireless client detected by an MSE.

**Note**

The Client Location report is not filtered in non-root virtual domain.

This section contains the following topics:

- [Configuring a Client Location Report, page 9-10](#)
- [Client Location Results, page 9-10](#)

Configuring a Client Location Report

The client location history report results are available only in root domain. To configure a Client Location History Report, follow these steps:

Settings

- Report Title—If you plan to save this report, enter a report name.
- Report By—By default, Client MAC Address is selected.
- Report Criteria—Click **Edit** and enter a valid MAC address as the filter criteria.

**Note**

In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
 - Select the radio button and choose a period of time from the drop-down list.
 - Or
 - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **Calendar** icon to choose a date. Choose the hours and minutes from the drop-down lists.

**Note**

The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters.

Customize Report Form

The Customize Report form allows you to customize the report results.

**Note**

Fixed columns appear in blue font and cannot be moved to the available columns.

Client Location Results

The results of the Client Location History report contain the following information:

- Last Located—The time when the client was located.
- Client Location—Position of the client at the located time.
- MSE—Name of the MSE that located this client.
- User—The username of the client.
- Detecting Controllers—The IP address of the detecting controller.
- 802.11 State—The state of 802.11. It can be either Probing or Associated.
- IP Address—The IP address of the client.
- AP MAC Address—The MAC address of the associated access point.
- Authenticated—Whether authenticated or not. This can be either Yes or No.
- SSID—The SSID used by the client.
- Protocol—The protocol used to retrieve the information from the client.

**Note**

The location field in this report is a hyperlink and clicking that hyperlink shows the location of the client in the floor map at the located time.

Client Location Density

This report shows wireless clients and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

- [Configuring a Client Location Density Report, page 9-11](#)
- [Client Location Density Results, page 9-12](#)

Configuring a Client Location Density Report

This section describes how to configure a Client Location Density Report and contains the following topics:

- [“Settings” section on page 9-11](#)
- [“Schedule” section on page 9-12](#)
- [“Customize Report Form” section on page 9-12](#)

Settings

- Report Title—If you plan to save this report, enter a report name.
- Report by
 - MSE By Floor Area
 - MSE By Outdoor Area
 - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.



Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
 - Select the radio button and choose a period of time from the drop-down list.
- Or
- Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **calendar** icon to choose a date. Select the hours and minutes from the drop-down lists.



Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters.

Customize Report Form

The Customize Report form allows you to customize the report results.



Note Fixed columns appear in blue font and cannot be moved to the Available columns.

Client Location Density Results

The results of the Client Location Density report contain the following information:

- Last Located—The time when the client was last located during the selected Report Time criteria.
- MAC Address—The MAC address of the client.
- Client Location—Position of the client at the located time.
- MSE—Name of the MSE that located this client.
- User—The username of the client.
- Detecting Controllers—The IP address of the detecting controller.
- 802.11 State—The state of 802.11. It can be either Probing or Associated.
- IP Address—The IP address of the client.
- SSID—The SSID used by the client.
- Protocol—The protocol used to retrieve the information from the client.



Note The location field in this report is a hyperlink and clicking that hyperlink shows the location of the client in the floor map at the located time.

Device Count by Zone

This report provides the count of devices detected by an MSE in the selected zone. This section contains the following topics:

This sections contains the following topics:

- [Configuring a Device Count by zone Report, page 9-13](#)
- [Device Count by Zone Results, page 9-14](#)

Configuring a Device Count by zone Report

This section describes how to configure a Device Count by Zone Report and contains the following topics:

- [Settings, page 9-13](#)
- [Schedule, page 9-14](#)
- [Customize Report Form, page 9-14](#)

Settings

- Report Title—If you plan to save this report, enter a report name.
- Report By
 - Indoor Area
 - Outdoor Area
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.



Note In the Report Criteria page, click **Select** to confirm your criteria or **Close** to return to the previous page.

- Device Type
 - All
 - Clients
 - Tags
 - RogueClients
 - Rogue APs
 - Interferers
 - Reporting Period
 - Select the radio button and choose a period of time from the drop-down list.
- or
- Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **Calendar** icon to choose a date. Select the hours and minutes from the drop-down lists.



Note The reporting period is based on the alarm last seen. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters.

Customize Report Form

The Customize Report form allows you to customize the report results.



Note Fixed columns appear in blue font and cannot be moved to the Available columns.

Device Count by Zone Results

The results of the Device Count by Zone report contains the following information:

- MSE—Name of the MSE that located this client.
- Zone—Device Count by Zone Results
- Device Type—Type of the device
- MSE Analytics Report Link—Link to get the MSE Analytics report

Device Dwell Time by Zone

This report provides the Dwell Time Report for a device detected by an MSE. This section contains the following topics:

This sections contains the following topics:

- [Configuring a Device Count by zone Report, page 9-13](#)
- Device Count by Zone Results

Configuring a Device Dwell Time by zone Report

This section describes how to configure a Device Dwell Count Time by Zone Report and contains the following topics:

- [Settings, page 9-13](#)
- [Schedule, page 9-14](#)
- [Customize Report Form, page 9-14](#)

Settings

- Report Title—If you plan to save this report, enter a report name.
- Report By
 - Indoor Area

- Outdoor Area
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.



Note In the Report Criteria page, click **Select** to confirm your criteria or **Close** to return to the previous page.

- Device Type
 - All
 - Client
 - Tags
 - Rogue Clients
 - Rogue APs
 - Interferers
 - Reporting Period
 - Select the radio button and choose a period of time from the drop-down list.
- or
- Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **Calendar** icon to choose a date. Select the hours and minutes from the drop-down lists.



Note The reporting period is based on the alarm last seen. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters.

Customize Report Form

The Customize Report form allows you to customize the report results.



Note Fixed columns appear in blue font and cannot be moved to the Available columns.

Device Dwell Time by Zone Results

The results of the Device Dwell Time by Zone report contains the following information:

- MSE—Name of the MSE that located this client.
- Zone—Device Count by Zone Results
- Device Type—Type of the device
- MSE Analytics Report Link—Link to get the MSE analytics report.

Guest Location Density

This report shows Guest clients and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

- [Configuring Guest Location Tracking, page 9-16](#)
- [Guest Location Tracking Results, page 9-17](#)

Configuring Guest Location Tracking

This section describes how to configure a Guest Location Tracking report and contains the following topics:

- [“Settings” section on page 9-16](#)
- [“Schedule” section on page 9-16](#)
- [“Customize Report Form” section on page 9-17](#)

Settings

- Report Title—If you plan to save this report, enter a report name.
- Report by
 - MSE By Floor Area
 - MSE By Outdoor Area
 - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.



Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
 - Select the radio button and choose a period of time from the drop-down list.
 - Or
 - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **Calendar** icon to choose a date. Choose the hours and minutes from the drop-down lists.



Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters.

Customize Report Form

The Customize Report form allows you to customize the report results.

**Note**

Fixed columns appear in blue font and cannot be moved to the Available columns.

Guest Location Tracking Results

The results of the Guest Location Tracking report contain the following information:

- Last Located—The time when the Guest client was last located during the selected Report Time criteria.
- Guest Username—The login name of the guest client user.
- MAC Address—The MAC address of the guest client.
- Guest Location—Position of the guest client at the located time.
- MSE—Name of the MSE that located this guest client.
- Detecting Controllers—The IP address of the detecting controller.
- IP Address—The IP address of the guest client.
- AP MAC Address—The MAC address of the access point to which the guest client is associated with.
- SSID—The SSID used by the guest client.
- Protocol—The protocol used to retrieve the information from the guest client.

**Note**

The location field in this report is a hyperlink and clicking that hyperlink shows the location of the guest in the floor map at the located time.

Location Notifications by Zone

This report shows Context-Aware notifications generated by MSEs. This report allows you to get missing device and device in/out notifications by the MSE, floor area, and outdoor area. This report is generated using CAS notifications and MSE notifications stored in the Prime Infrastructure database.

**Note**

This report is not filtered in non-root virtual domain.

This section contains the following topics:

- [Configuring a Location Notification Report, page 9-17](#)
- [Location Notification Results, page 9-19](#)

Configuring a Location Notification Report

- This section describes how to configure a Location Notification report and contains the following topics:
- [Schedule, page 9-18](#)

- [Customize Report Form, page 9-18](#)

Settings

- Report Title—If you plan to save this report, enter a report name.
- Report by
 - Missing Device Notifications by MSE
 - Missing Device Notifications by Floor Area
 - Missing Device Notifications by Outdoor Area
 - Device In/Out Notifications by MSE
 - Device In/Out Notifications by Floor Area
 - Device In/Out Notifications by Outdoor Area
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.



Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Device Type
 - All
 - Client
 - Tag
 - Rogue Client
 - Rogue AP
 - Interferer
- Reporting Period
 - Select the radio button and choose a period of time from the drop-down list.
 - Or
 - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box or click the **calendar** icon to choose a date. Choose the hours and minutes from the drop-down lists.



Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters.

Customize Report Form

The Customize Report form allows you to customize the report results.

**Note**

Fixed columns appear in blue font and cannot be moved to the Available columns.

Location Notification Results

The results of the Location Notification report contain the following information:

- Last Seen—The date and time when the device was last located.
- MAC Address—The MAC address of the device.
- Device Type—The type of the device.
- Asset Name—The name of the asset.
- Asset Group—The name of the asset group.
- Asset Category—The name of the asset category.
- Map Location—The map location where the device was located.
- ServerName—The name of the server that sends the ContextAware notifications.

Mobile MAC Statistics

This report shows the most active Mobile Mac addressed based on click count by MSAP servers or by venues.

- [Configuring Rogue AP Location Tracking, page 9-21](#)
- [Rogue AP Location Tracking Results, page 9-21](#)

Configuring Mobile MAC Statistics

This section describes how to configure a Mobile MAC Statistics report and contains the following topics:

- [“Settings” section on page 9-21](#)
- [“Schedule” section on page 9-21](#)
- [“Customize Report Form” section on page 9-21](#)

Settings

- Report Title—If you plan to save this report, enter a report name.
- Report by
 - MSE By Floor Area
 - MSE By Outdoor Area
 - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.



Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
 - Select the radio button and choose a period of time from the drop-down list.
 - Or
 - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **calendar** icon to choose a date. Choose the hours and minutes from the drop-down lists.



Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters.

Customize Report Form

The Customize Report form allows you to customize the report results.



Note Fixed columns appear in blue font and cannot be moved to the Available columns.

Mobile MAC Statistics

The results of the Mobile MAC Statistics report contain the following information:

- Venue
- Click Count
- Mobile MAC Address



Note The location field in this report is a hyperlink and clicking that hyperlink shows the location of the rogue AP in the floor map at the located time.

Rogue AP Location Density

This report shows Rogue APs and their locations detected by the MSEs based on your filtering criteria.

This section contains the following topics:

- [Configuring Rogue AP Location Tracking, page 9-21](#)
- [Rogue AP Location Tracking Results, page 9-21](#)

Configuring Rogue AP Location Tracking

This section describes how to configure a Rogue AP Location Tracking report and contains the following topics:

- “Settings” section on page 9-21
- “Schedule” section on page 9-21
- “Customize Report Form” section on page 9-21

Settings

- Report Title—If you plan to save this report, enter a report name.
- Report by
 - MSE By Floor Area
 - MSE By Outdoor Area
 - MSE
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and select the required filter criteria.



Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
 - Select the radio button and choose a period of time from the drop-down list.
 - Or
 - Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **calendar** icon to choose a date. Choose the hours and minutes from the drop-down lists.



Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters.

Customize Report Form

The Customize Report form allows you to customize the report results.



Note

Fixed columns appear in blue font and cannot be moved to the Available columns.

Rogue AP Location Tracking Results

The results of the Rogue AP Location Tracking report contain the following information:

- Last Located—The time when the Rogue AP was last located during the selected Report Time criteria.
- MAC Address—The MAC address of the rogue access point.
- Rogue AP Location—Position of the Rogue AP at the located time.
- MSE—Name of the MSE that located this Rogue AP.
- State—The state of the Rogue AP.

**Note**

The location field in this report is a hyperlink and clicking that hyperlink shows the location of the rogue AP in the floor map at the located time.

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 one of these protocols: **All Clients**, **All Wired (802.3)**, **All Wireless (802.11)**, **802.11a/n**, **802.11b/g/n**, **802.11a**, **802.11b**, **802.11g**, **802.11n (5-GHz)**, or **802.11n (2.4-GHz)**.
- SSID—All SSIDs is the default value.
- 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 list boxes.

Step 10 Select the **Recurrence** radio button to determine how often you want to run the report. The possible values are:

- 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 [Step 10](#), 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 you entered.



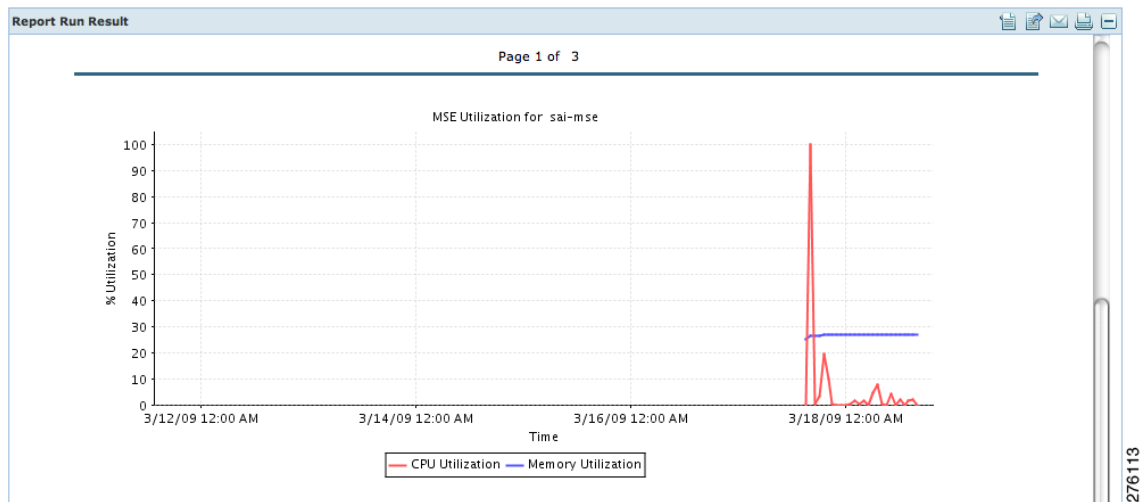
Note You can also click **Run Now** to check the defined report criteria before saving it or to run reports as necessary.

The results appear at the bottom of the page (see [Figure 9-2](#)).



Note Only the CPU and memory utilization reports are shown in the following example (see [Figure 9-2](#)).

Figure 9-2 *Devise > MSE Utilization > Results*



Step 12 If you selected the Save or Save and Run option, choose either **Reports > Saved Reports** (or **Reports > Scheduled Runs** if the report has not yet run and is scheduled to run). The Utilization Reports Summary page appears.

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 13 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 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.

Security Reports and Alarms for wIPS

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

**Note**

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

The choices are as follows:

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

**Note**

This report was formally called the Rogue Detected by AP.

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

This section contains the following topics:

- [Creating a New wIPS Security or Alarms Report, page 9-25](#)
- [Viewing a Saved wIPS Report, page 9-27](#)
- [Viewing Scheduled wIPS Report Runs, page 9-27](#)

Creating a New wIPS Security or Alarms Report

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

To create a new security report, follow these steps:

**Note**

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

-
- Step 1** Choose **Reports > Report Launch Pad**. The Report Launch Pad page appears.
- Step 2** Choose **Security** and click one of the report types in the left pane (such as Adaptive wIPS Top 10 Report Details).
- Step 3** Click **New**. The New report page appears.
- Step 4** In the Settings pane, enter a report title.
- Step 5** The Report By is, by default, MSE with Adaptive wIPS Service.
- Step 6** The Report Criteria is always either a specific mobility services engine or All MSEs with Adaptive wIPS Service.
- Step 7** Click **Edit** to add or modify the Report Criteria. The Filter Criteria dialog box appears.
- Step 8** Enter the reporting period. You can define the report to collect data hourly, weekly, or at a specific date and time. The selected reporting period type 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 9** In the Schedule pane, select the **Enable Schedule** check box.
- Step 10** Choose the report format (CSV or PDF) from the Export Report drop-down list.
- Step 11** Select either **File** or **Email** as the destination of the report.
- If you select the File option, a destination path must first be defined 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 12** Enter a start date (MM:DD:YYYY), or click the **calendar** icon to select a date.
- Step 13** Choose a start time using the hour and minute drop-down lists.
- Step 14** Select any one of the Recurrence options to determine how often the report is to be run.



Note The days of the week check boxes appear when you select **Weekly** radio button.

You can also use the Customize Report option to customize the report. Click **Customize** and provide the required information to generate the report.

- Step 15** When you have completed [Step 1](#) to [Step 14](#), 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 pane.
 - Click **Save and Run** to save the changes and run the report now. The report runs regardless of any pending, scheduled run of that report. Results appear the bottom of the 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 pane.
 - 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 NCS 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 you entered.



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

The results appear at the bottom of the page.

Step 16 Repeat [Step 2](#) to [Step 15](#) for each wIPS report you want to create.

Viewing a Saved wIPS Report

To download a saved report, follow these steps:

-
- Step 1** Choose **Reports > Saved Reports**.
- Step 2** Click the History icon to see the date of the last report run.
- Step 3** Click the **Download** icon for your request. It is downloaded and saved in the defined directory or e-mailed.
-

Viewing Scheduled wIPS Report Runs

To review 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.

This section contains the following topics:

- [Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address, page 9-28](#)
- [Viewing the Clients Detected by the MSE, page 9-29](#)

Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address



Note Only wireless clients have IPv6 addresses in this release.

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 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 controllers. This list of clients should be the same as that is displayed in Monitor > Clients and Users page. If the floors are not assigned to a virtual domain, the client list is empty. If a floor is assigned to a virtual domain but not synchronized with the MSE, then the clients from that floor is not be displayed.

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 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 the 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 the 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 the MSE by choosing **Clients detected by MSE** from the Show drop-down list.

All the clients detected by the 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.
 -  Indicates a lightweight client
 -  Indicates a wired client
 -  Indicates an autonomous client
- Vendor—Device vendor derived from OUI.
- Device Name—Network authentication device name. For example, WLC and switch.
- Location—Map location of the connected device.
- VLAN—Indicates the access VLAN ID for this client.
- Status—Current client status.
 - Idle—Normal operation; no rejection of client association requests.
 - Auth Pending—Completing a AAA transaction.
 - Authenticated—802.11 authenticated complete.
 - Associated—802.11 association complete. This is also used by wired clients to represent that a client is currently connected to the network.
 - Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.
 - To Be Deleted—The client is deleted after disassociation.
 - Excluded—Automatically disabled by the system due to perceived security threat.
- Interface—Controller interface (wireless) or switch interface (wired) that the client is connected to.
- Protocol
 - 802.11—Wireless
 - 802.3—Wired
- Association Time—Last association start time (for wireless client). For a wired client, this is the time when a client is connected to a switch port. This is blank for a client which is associated but has problems being on the network.
- CCX—Lightweight wireless only.

Step 3 Select the radio button next to MAC Address in the Client and User page to view the associated client information. The following are the different client parameters that appear.

- [Client attributes](#)
- Client IPV6 Addresses
- Client Statistics



Note Client Statistics shows the statistics information after the client details are shown.


- Client Association History
- Client Event Information
- Client Location Information
- Wired Location History
- Client CCX Information

Client Attributes

When you select a client from the Clients and Users list, the following client details are displayed. Clients are identified using the MAC address.

- General—Lists the following information:
 - User Name
 - IP Address
 - MAC address
 - Vendor
 - Endpoint Type
 - Client Type
 - Media Type
 - Mobility Role
 - Hostname
 - E2E
 - Power Save
 - CCX
 - Foundation Service
 - Management Service
 - Voice Service
 - Location Service



Note Click the  icon next to the username to access the correlated users of a user.

- Session—Lists the following client session information:
 - Controller Name
 - AP Name

- AP IP Address
- AP Type
- AP Base Radio MAC
- Anchor Address
- 802.11 State
- Association ID
- Port
- Interface
- SSID
- Profile Name
- Protocol
- VLAN ID
- AP Mode
- Security (wireless and Identity wired clients only)—Lists the following security information:
 - Security Policy Type
 - EAP Type
 - On Network
 - 802.11 Authentication
 - Encryption Cipher
 - SNMP NAC State
 - RADIUS NAC State
 - AAA Override ACL Name
 - AAA Override ACL Applied Status
 - Redirect URL
 - ACL Name
 - ACL Applied Status
 - FlexConnect Local Authentication
 - Policy Manager State
 - Authentication ISE
 - Authorization Profile Name
 - Posture Status
 - TrustSec Security Group
 - Windows AD Domain



Note The identity clients are 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 controller. 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 dashlet shows information regarding the last ten association times for the selected client. This information helps in troubleshooting the client.

The Association History dashlet contains the following information:

- Association Time
- Duration
- User Name
- IP Address
- IP Address Type
- AP Name
- Controller Name
- SSID

Events

The 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
-

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.

This section contains the following topics:

- [Adding a Building to a Campus Map, page 9-34](#)
- [Viewing a Building, page 9-37](#)
- [Editing a Building, page 9-38](#)
- [Deleting a Building, page 9-38](#)
- [Moving a Building, page 9-39](#)

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 **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:
- Enter the building name.
 - Enter the building contact name.
 - Enter the number of floors and basements.
 - 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.

- 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.

- 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.
- 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.

- Click **Save** to save this building and its campus location to the database. The Prime Infrastructure 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:
- 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**, 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.
- 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.



Note Each selected parameter 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 parameter, 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](#)” section on page 9-34 for more information.
- Edit Building—See the “[Editing a Building](#)” section on page 9-38 for more information.
- Delete Building—See the “[Deleting a Building](#)” section on page 9-38 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**.
-
-

- Step 8** Tags detected by MSE (in last 15 mins) displays total tags count equal to the number of tags by floors in the given virtual domain. The RFID Tags Summary page displays list of tags by floors in the given domain.



Note If the floors are not assigned to a virtual domain, then the tag count will be zero. If a floor is assigned to a virtual domain but not synchronized with the MSE, then the tag count from that floor is not considered.

This list of tags are the same as that is displayed in Monitor > RFID Tags summary page. If the floors are not assigned to a virtual domain, the tags list shows empty. If the floor is assigned to a virtual domain and is not synchronized with the MSE, then the tags from that floor is not displayed.

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.

If the existing chokepoints are on a floor, then they all belong to the same virtual domain as the floor. If the chokepoints are not placed on a floor, then they are available in all virtual domains. This list should display chokepoints belonging to the current virtual domain. Chokepoints that are not placed on a floor belong to all virtual domains. If a chokepoint is placed on a floor, it should be displayed in the same virtual domain as the floor on which it is placed.

When a new TDOA receiver 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 the floor. When a TDOA receiver is removed from a floor, it will be available in all the virtual domains again.

If the existing TDOA receivers are on a floor, then they all belong to the same virtual domain as the floor. If the chokepoints are not placed on a floor, then they are available in all virtual domains. This list displays Wi-Fi TDoA receivers belonging to the current virtual domain. The Wi-Fi TDoA receivers that are not placed on a floor is belonged to all the virtual domains. If a Wi-Fi TDoA receivers is placed on a floor, it should be displayed in the same virtual domain as the floor on which it is placed.

Monitoring Geo-Location

The MSE provides physical location of wired clients, wired end points, switches, controllers, 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 of 3 GPS markers are required for geo-location calculation. The maximum number of GPS markers that you can add is 20.

This section contains the following topics:

- [Adding a GPS Marker to a Floor Map, page 9-40](#)
- [Editing a GPS Marker, page 9-41](#)
- [Deleting a GPS Marker Present on a Floor, page 9-41](#)

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 the **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.
- Step 4** Select an existing GPS marker present on the floor.
- 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 Present on a Floor

To delete a GPS marker present on a 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.



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.



CHAPTER 10

MSAP

Cisco Mobility Services Advertisement Protocol (MSAP) provides requirements for MSAP clients and servers and describes the message exchanges between them. Mobile devices can retrieve service advertisements from an MSAP server over Wi-Fi infrastructure using MSAP. MSAP is introduced in this release of the mobility services engine (MSE) and provides server functionality.

MSAP is used by the mobile devices that have been configured with a set of policies for establishing network connectivity. MSAP facilitates mobile devices to discover network-based services available in a local network or services that are enabled through service providers. MSAP provides service advertisements that describe available services to mobile devices. Once the mobile device receives the service advertisements, it displays their icon and data on its user interface. You can launch the advertised service by clicking the displayed icon.



Note

The MSAP is available only in the root virtual domain from 7.3 Release.

This chapter contains the following sections:

- [Licensing for MSAP, page 10-1](#)
- [Provisioning MSAP Service Advertisements, page 10-2](#)
- [Deleting Service Advertisements, page 10-4](#)
- [Applying Service Advertisements to a Venue, page 10-4](#)
- [Viewing the Configured Service Advertisements per MSE, page 10-5](#)
- [Viewing MSAP Statistics, page 10-5](#)
- [Viewing the MSE Summary Page for MSAP License Information, page 10-6](#)
- [Viewing Service Advertisements Synchronization Status, page 10-6](#)
- [MSAP Reports, page 10-6](#)

Licensing for MSAP

The MSAP license is based on the number of service advertisements supported by the MSE. There is only an evaluation license available for MSAP with a limit of 1000 service advertisement clicks.

Provisioning MSAP Service Advertisements

To add new MSAP advertisements, follow these steps:



Note The **Services > MSAP** page is available only in root virtual domain.

- Step 1** Choose **Services > MSAP**.
- Step 2** From the Select a command drop-down list, choose **Add Service Advertisements**, and click **Go**.
The Service Advertisement Details page appears.
- Step 3** Enter the service provider name in the Provider Name text box. This is the name of the provider who wants to provide advertisements to the client.
- Step 4** Select an icon that is associated with the service provider by clicking **Choose File**. This is the icon that is displayed on the client handset.

Adding Venue Policy to Service Advertisements



Note You can also apply service advertisements to a venue by choosing **Services > MASP**. See the [“Applying Service Advertisements to a Venue”](#) section on page 10-4 for more information on how to apply service advertisements.

- Step 5** Click **Add Venue** to specify at which venues you want the advertisements to be broadcasted.
The Add/Edit Venue page appears.
- Step 6** Enter the venue name in the Venue Name text box.
- Step 7** From the Area Type drop-down list, choose the area type where you want to display the service advertisements. The possible values are **Floor Area** and **Outdoor area**.
- Step 8** From the Campus drop-down list, choose the campus name where you want to display the service advertisements.
- Step 9** From the Building drop-down list, choose the building name where you want the advertisements to appear.
- Step 10** From the Floor drop-down list, choose the floor type.



Note Depending on what floor you choose, the information in the Display near selected APs information changes.

- Step 11** From the Coverage area drop-down list, choose the coverage area with the floor.
- Step 12** From the SSID drop-down list, choose the SSIDs on which you want to broadcast the service advertisements. You can choose multiple SSIDs.
- Step 13** Select the Display Rule radio button. You can select either the **Display everywhere** or **Display near selected APs** radio button. By default, Display everywhere is selected.

If you select Display everywhere, then it searches for all the MSAP-supported controllers that provide these SSIDs and assigns these controllers to the MSE.

If you select Display near selected APs, then you can configure the following parameters:

- AP—Select those APs on which you want the advertisements to broadcast.

- **Radio**—Select the radio frequency on which you want the advertisements to be broadcasted. The service advertisement is displayed when the mobile device is near the radio band that you have selected. The possible values are 2.4 GHz or 5 GHz.
 - **min RSSI**—Enter a value for RSSI at which you want the service advertisements to be displayed on the user interface.
- Step 14** Click **Save** to add the venue. The venue is added to the list of venues in the Service Advertisement Details page.

Adding Service Brief Information to the Service Advertisement

- Step 15** Click **Add Advertisement**.
- The Add/Edit Advertisement page appears.
- Step 16** From the Advertisement Type drop-down list, choose the type of advertisement you want to display.
- Step 17** Enter the name that you want to display on the handset in the Friendly Name text box.
- Step 18** Enter the service description in the Friendly Description text box.
- Step 19** Enter the URL for each type of handset. The URL identifies the location at which the service can be retrieved. You can add multiple URLs by clicking **Add More URL**.
- Step 20** Click **Save**. This information is applied to the MSE and the synchronization happens automatically.
-

Adding Service Advertisements to the Floor Map

To add service advertisements to a coverage area within the floor map, follow these steps:

-
- Step 1** Choose Monitor > Site Maps.
- The Site Maps page is displayed.
- Step 2** Choose the appropriate floor location link from the list.
- A map appears showing the placement of all installed access points, client, and tags and their relative signal strength.
- Step 3** Click on Services icon on the floor map page.
- The Venue dialog box to associate service advertisement to that particular venue is displayed.
- Step 4** Click on Show/Associate Services link to open the Add/Edit MSAP Services.
- The list of all the available service advertisements are displayed and you can associate service advertisements by selecting them.
- Step 5** To associate a service advertisement, you can do the following:
- You can select an advertisement by filtering based on either provider name or friendly name by selecting them from the Filter By drop down list.
 - or
 - You can click on Associate check box to associate that particular service advertisement.
- Step 6** Click OK.
-

Creating Service Advertisements from the Floor Map

To create service advertisements from the floor map, follow these steps:

-
- Step 1** Choose Monitor > Site Maps.
The Site Maps page is displayed.
 - Step 2** Choose the appropriate floor location link from the list.
A map appears showing the placement of all installed access points, client, and tags and their relative signal strength.
 - Step 3** Click on Services icon on the floor map page.
The Venue dialog box to associate service advertisement to that particular venue is displayed.
 - Step 4** Click on Show/Associate Services link to open the Add/Edit MSAP Services.
The list of all the available service advertisements are displayed and you can associate service advertisements by selecting them.
 - Step 5** Click Create MSAP Service to create service advertisements.
It redirects you to Service > MSAP > Add Service Advertisements page.
 - Step 6** Follow steps given in [Provisioning MSAP Service Advertisements, page 10-2](#) to create service advertisements.
-

Deleting Service Advertisements

To delete a service advertisement, follow these steps:

-
- Step 1** Choose **Services > MSAP**.
The MSAP page appears.
 - Step 2** Select the check box of the service advertisement that you want to delete.
 - Step 3** From the Select a command drop-down list, choose **Delete Service Advertisement**, and click **Go**, or Click **Delete** in the MSAP page.
 - Step 4** Click **OK** to confirm the deletion.
-

Applying Service Advertisements to a Venue

To apply service advertisements to a venue, follow these steps:

-
- Step 1** Choose **Services > MSAP**.
 - Step 2** Select the check box of the service advertisement that you to apply to a venue.
 - Step 3** From the Select a command drop-down list, choose **Apply to Venue(s)**.
 - Step 4** Click **Go**.

- Step 5** Follow [Step 6](#) through [Step 14](#) in the “[Provisioning MSAP Service Advertisements](#)” section on [page 10-2](#).
- or
- Click **Apply to Venues** in the MSAP page and follow [Step 6](#) through [Step 14](#) in the “[Provisioning MSAP Service Advertisements](#)” section on [page 10-2](#).
-

Viewing the Configured Service Advertisements per MSE

To view the configured service advertisements per MSE, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engine**.
- Step 2** Click **Device Name** to view its properties.
The General Properties page appears.
- Step 3** Choose **MSAP Service > Advertisements** from the left sidebar menu.
The following information appears in the MSAP Service page:
- Icon—Displays an icon associated with the service provider.
 - Provide Name—Displays the service providers name.
 - Venue Name—Displays the venue name.
 - Advertisements
 - Friendly Name—Friendly name that is displayed on the handset.
 - Advertisement Type—Type of advertisement that is displayed on the handset.
-

Viewing MSAP Statistics

To view MSAP statistics, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engine**.
- Step 2** Click **Device Name** to view its properties.
The General Properties page appears.
- Step 3** Choose **MSAP Service > Statistics** from the left sidebar menu.
The following information appears in the MSAP Service page:
- Top 5 Active Mobile MAC addresses—Displays information about the most active mobiles in a given venue.
 - Top 5 Service URIs—Displays information about the usage of the services across a given venue or provider.
-

Viewing the MSE Summary Page for MSAP License Information

For more information about MSE licensing, see the Mobility Services Engine (MSE) License Summary section in the *Cisco Prime Infrastructure Configuration Guide*.

Viewing Service Advertisements Synchronization Status

To view service advertisements synchronization status, follow these steps:

-
- Step 1** Choose **Services > Synchronize Services**.
- Step 2** Choose **Service Advertisements** from the left sidebar menu. The following information appears in the Service Advertisements page.
- **Provider Name**—Shows the name of the service provider.
 - **Service**—Shows the type of service that a particular advertisement is using.
 - **MSE**—Shows whether the service advertisement is synchronized with the MSE or not.
 - **Sync Status**—Shows the synchronization status. A green two-arrow icon indicates that its corresponding element is synchronized with the given server such as MSE. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a given server.
 - **Message**—Shows any message related to the advertisement synchronization failure.
-

MSAP Reports

This section describes how to create the MSAP reports and contains the following topics:

- [Mobile MAC Statistics, page 10-6](#)
- [Service URI Statistics, page 10-7](#)

Mobile MAC Statistics

Click **Mobile MAC Statistics** from the Report Launch Pad to open the Mobile MAC Statistics Reports page. In this page, you can enable, disable, delete, or run currently saved report templates.

To create a new report, click **New** in the Report Launch Pad page or in the Mobile MAC Statistics Reports page. See the “[Configuring a Mobile MAC Statistics Report](#)” section on [page 10-6](#) for more information.

Configuring a Mobile MAC Statistics Report

This section describes how to configure an Mobile MAC Statistics report.

Settings

- **Report Title**—If you want to save this report template, enter a report name.
- **Report by**

- Mobile MAC by MSAP Server—Choose this option if you want to generate a report on mobile MACs based on MSAP servers.
- Mobile MAC by Venue—Choose this option if you want to generate a report on mobile MACs based on venue.
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and choose the required filter criteria.



Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
 - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
 - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.



Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.



Note Fixed columns appear in blue font and cannot be moved to the Available columns.

The Mobile MAC Statistics report results contain the following:

- Mobile MAC
- Click Count



Note This report provides Most Active Mobile MACs based on click count by MSE and/or by venue. If multiple MSEs are selected, top Mobile MACs are grouped by each MSE in the selected sorting order.

Service URI Statistics

Click **Service URI Statistics** in the Report Launch Pad page to open the Service URI Statistics Reports page. In this page, you can enable, disable, delete, or run currently saved report templates.

To create a new report, click **New** from the Report Launch Pad or from the Mobile MAC Statistics Reports page. See the [“Configuring a Service URI Statistics Report”](#) section on page 10-7 for more information.

Configuring a Service URI Statistics Report

This section describes how to configure an Service URI Statistics report.

Settings

- Report Title—If you plan to save this report template, enter a report name.
- Report by

- Service URI by MSAP Server—Choose this option if you want to generate a report on mobile MACs based on MSAP servers.
 - Service URI by Venue—Choose this option if you want to generate a report on the Service URIs based on Venue.
 - Service URI by Mobile MAC—Choose this option if you want to generate a report on the Service URIs based on Mobile MAC.
 - Service URI by Provider—Choose this option if you want to generate a report on the Service URIs based on Provider.
- Report Criteria—The report criteria differs based on the Report By option selected. Click **Edit** and choose the required filter criteria.



Note In the Report Criteria page, click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Reporting Period
 - Last—Select the **Last** radio button and choose a period of time from the drop-down list.
 - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **calendar** icon to choose a date. Choose the hours and minutes from the drop-down lists.



Note The reporting period is based on the alarm last seen time. The times are in the UTC time zone.



Note Fixed columns appear in blue font and cannot be moved to the Available columns.

The Service URI Statistics report results contain the following:

- Service URI
 - Mobile MAC
 - Click Count
 - This report provides Top Service URIs based on click count by MSE and/or by venue. If the multiple MSEs are selected, top Service URIs are grouped by each MSE in the selected sorting order.
-



CHAPTER 11

Performing Maintenance Operations

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

This chapter contains the following sections:

- [Guidelines and Limitations, page 11-1](#)
- [Recovering a Lost Password, page 11-1](#)
- [Recovering a Lost Root Password, page 11-2](#)
- [Backing Up and Restoring Mobility Services Engine Data, page 11-2](#)
- [Downloading Software to the Mobility Services Engines, page 11-4](#)
- [Configuring the NTP Server, page 11-6](#)
- [Resetting the System, page 11-6](#)
- [Clearing the Configuration File, page 11-6](#)

Guidelines and Limitations

- Ensure that you remember the password and change the password only if it is absolutely necessary.
- While recovering a lost root password, the shell prompt does not appear if you set up a single-user mode password.

Recovering a Lost Password

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

-
- Step 1** When the GRUB page appears, press **Esc** to enter the boot menu.
 - Step 2** Press **e** to edit.
 - Step 3** Navigate to the line beginning with kernel and press **e**.
At the end of the line, put a space, followed by the number one (**1**). Press **Enter** to save this change.
 - Step 4** Press **b** to begin boot.
At the end of the boot sequence, a shell prompt appears.
 - Step 5** The user may change the root password by entering the **passwd** command.

- Step 6** Enter and confirm the new password.
- Step 7** Reboot the machine.
-

Recovering a Lost Root Password

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

- Step 1** When the GRUB page appears, press **Esc** to enter the boot menu.
- Step 2** Press **e** to edit.
- Step 3** Navigate to the line beginning with kernel and press **e**.
At the end of the line, enter a space, followed by the number one (**1**). Press **Enter** to save this change.
- Step 4** Press **b** to begin boot sequence.
At the end of the boot sequence, a shell prompt appears.



Note The shell prompt does not appear if you set up a single-user mode password.

- Step 5** You can change the root password by entering the **passwd** command.
- Step 6** Enter and confirm the new password.
- Step 7** Restart the machine.



Note Ensure that you remember the root password and only change the password if it is absolutely necessary.

Backing Up and Restoring Mobility Services Engine Data

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

This section contains the following topics:

- [Guidelines and Limitations, page 11-2](#)
- [Backing Up Mobility Services Engine Historical Data, page 11-3](#)
- [Restoring Mobility Services Engine Historical Data, page 11-3](#)
- [Enabling Automatic Location Data Backup, page 11-4](#)

Guidelines and Limitations

- Backups are stored in the FTP directory you specify during the Cisco Prime Infrastructure installation.

- You can run the backup process in the background while working on other mobility services engine operations in the other Prime Infrastructure page.

Backing Up Mobility Services Engine Historical Data

The Prime Infrastructure includes functionality for backing up mobility services engine data.

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

-
- Step 1** Choose **Services > Mobility Services**.
 - Step 2** Click the name of the mobility services engine that you want to back up.
 - Step 3** Choose **System > Maintenance**.
 - Step 4** Click **Backup**.
 - Step 5** Enter the name of the backup.
 - Step 6** Click **Submit** to back up the historical data to the hard drive of the server running the Prime Infrastructure.

The Status of the backup is visible on the page while the backup is in process. Three items appear in the page during the backup process: (1) Last Status text box that provides messages noting the status of the back up; (2) Progress text box that shows what percentage of the backup is complete; and (3) Started at text box that shows when the backup began noting date and time.



Note You can run the backup process in the background while working on other mobility services engine operations in the other Prime Infrastructure page.



Note Backups are stored in the FTP directory you specify during the Prime Infrastructure installation.

Restoring Mobility Services Engine Historical Data

You can use the Prime Infrastructure to historical data (from backup)

To restore mobility services engine data, follow these steps:

-
- Step 1** Choose **Services > Mobility Services**.
 - Step 2** Click the name of the mobility services engine that you want to restore.
 - Step 3** Choose **System > Maintenance**.
 - Step 4** Click **Restore**.
 - Step 5** Choose the file to restore from the drop-down list.
 - Step 6** Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the mobility services engine.

This option is applicable for network designs, wired switches, controllers, and event definitions. The existing location history data is retained, however, you must use manual service assignments to perform any future location calculations.

- Step 7** Click **Submit** to start the restoration process.
- Step 8** Click **OK** to confirm that you want to restore the data from the Prime Infrastructure server hard drive. When restoration is completed, the Prime Infrastructure displays a message to that effect.



Note You should not work on other mobility services engine operations when the restore process is running.

Enabling Automatic Location Data Backup

You can configure Prime Infrastructure to perform automatic backups of location data on a regular basis. To enable automatic backup of location data on a mobility services engine, follow these steps:

- Step 1** Choose **Administration > Background Tasks**.
- Step 2** Select the **Mobility Service Backup** check box.
- Step 3** From the Select a command drop-down list, choose **Enable Task**, and click **Go**.
- The backups are stored in the FTP directory that you specify during the Prime Infrastructure installation.

Downloading Software to the Mobility Services Engines

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

- Step 1** Verify that you can ping the mobility services engine from the Prime Infrastructure server or an external FTP server, whichever you are going to use for the application code download.
- Step 2** Choose **Services > Mobility Services Engine**.
- Step 3** Click the name of the mobility services engine to which you want to download software.
- Step 4** Choose **System > Maintenance > Download Software** from the left sidebar menu.
- Step 5** To download software, do one of the following:
- To download software listed in the Prime Infrastructure directory, select the **Select from uploaded images to transfer into the Server** radio button. Choose a binary image from the drop-down list. Prime Infrastructure downloads the binary image to the FTP server directory you specified during the Prime Infrastructure installation.
 - To use downloaded software available locally or over the network, select the **Browse a new software image to transfer into the Server** radio button and click **Choose File**. Locate the file and click **Open**.
- Step 6** Click **Download** to send the software to the /opt/installers directory on the mobility services engine.

- Step 7** After the image is transferred to the mobility services engine, log in to the mobility services engine command-line interface.
- Step 8** Run the installer image from the `/opt/installers` directory by entering the `./bin mse image` command. This installs the software.
- Step 9** To run the software, enter the `/etc/init.d/msed start` command.



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

Manually Downloading Software

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

- Step 1** Transfer the new mobility services engine image onto the hard drive.
- Log in as root, and use the binary setting to send the image from an external FTP server root directory. The release note format is similar to the following and changes with each release:
CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz.



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



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

Your entries should look like the following example:

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

- Verify that the image (CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz) is in the mobility services engine `/opt/installers` directory.
- To decompress (unzip) the image file, enter the following command:
gunzip CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz
The decompression yields a bin file.
- Make sure that the CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz file has execute permissions for the root user. If not, enter the following command:

```
chmod 755 CISCO-MSE-L-K9-x-x-x-x.bin.
```

Step 2 Manually stop the mobility services engine.

Step 3 Log in as root and enter the following command:

```
/etc/init.d/msed stop.
```

Step 4 To install the new mobility services engine image, enter the following command:

```
/opt/installers/CISCO-MSE-L-K9-x-x-x-x.bin.
```

Step 5 Start the new mobility services engine software by entering the following command:

```
/etc/init.d/msed start
```



Caution

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

Step 6 Enter the following command to uninstall the script files of the mobility services engine:

```
/opt/mse/uninstall
```

Configuring the NTP Server

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



Note

- You are automatically prompted to enable NTP and enter NTP server IP addresses as part of the automatic installation script for the mobility services engine. For more details on the automatic installation script, see the *Cisco 3350 Mobility Services Engine Getting Started Guide* or *Cisco 3310 Mobility Services Engine Getting Started Guide* at the following URL:

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

- If you need to add or change an NTP server installation after a mobility services engine install, rerun the automatic installation script. You can configure the NTP server without adjusting the other values by tabbing through the script.



Note

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

Resetting the System

For information on rebooting or shutting down the mobility services engine hardware, see the “[Rebooting or Shutting Down a System](#)” section on page 6-10.

Clearing the Configuration File

For information on clearing the configuration file, see the “[Clearing the System Database](#)” section on page 6-10.



CHAPTER **A**

wIPS Policy Alarm Encyclopedia

This appendix provides an overview of the threat types addressed by wIPS and contains the following sections:

- [Security IDS/IPS Overview, page A-1](#)
- [Intrusion Detection—Denial of Service Attack, page A-2](#)

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 underestimate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured and unconfigured access points and DoS (denial of service) attacks.

The Cisco Adaptive Wireless IPS (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

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.

Preconfigured Profiles for Various WLAN Environments

During installation, the user can select an appropriate profile based on the WLAN network implemented.

The wIPS provides separate profiles for the following:

- Enterprise best practice

- Enterprise rogue detection only
- Financial (Gramm-Leach-Bliley Act compliant)
- HealthCare (Health Insurance Portability and Accountability Act compliant)
- Hotspot implementing 802.1x security
- Hotspot implementing NO security
- Tradeshow environment
- Warehouse/manufacturing environment
- Government/Military (8100.2 directive compliant)
- Retail environment

When you select the appropriate profile, the wIPS enables or disables alarms from the policy profile that are appropriate for that WLAN environment. For example, health care institutions can select the Healthcare profile and all alarms that are necessary to be HIPAA compliant are enabled. The administrator still has the option after installation to enable or disable any alarm or change the threshold values as per individual preferences.

Not only is the wIPS system an IDS (Intrusion Detection System), but it is also an IPS (Intrusion Prevention System).

Cisco Adaptive Wireless IPS policies are included in two security subcategories: wIPS—denial of service (DoS) Attacks and wIPS—Security Penetration.

This section contains the following topics:

- [Intrusion Detection—Denial of Service Attack, page A-2](#)
- [Intrusion Detection—Security Penetration, page A-23](#)

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 NCS 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.

This section describes the three denial of service attacks subcategories and contains the following topics:

- [Denial of Service Attacks Against Access Points, page A-3](#)
- [Denial of Service Attack Against Infrastructure, page A-8](#)

- [Denial of Service Attacks Against Client Station, page A-13](#)

Denial of Service Attacks 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 NCS online Help.

This section describes DoS attacks against access points and contains the following topics:

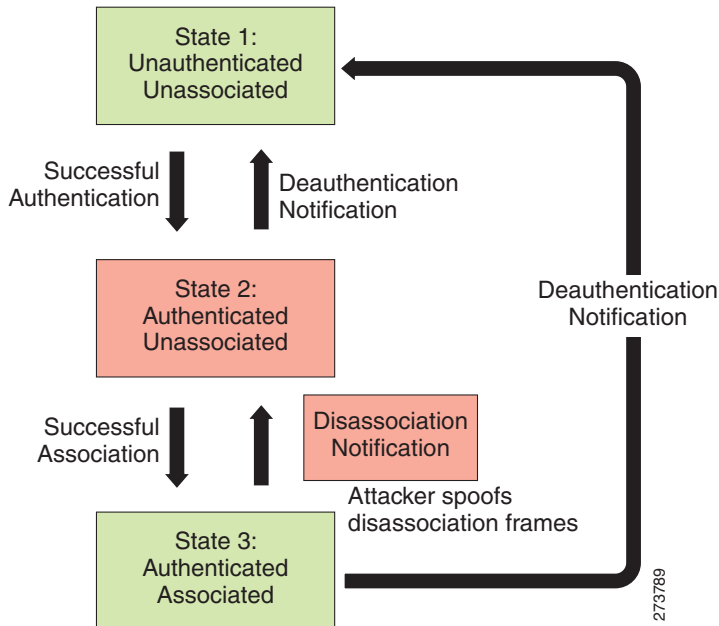
- [Denial of Service Attack: Association Flood, page A-3](#)
- [Denial of Service Attack: Association Table Overflow, page A-4](#)
- [Denial of Service Attack: Authentication Flood, page A-5](#)
- [Denial of Service Attack: EAPOL-Start Attack, page A-6](#)
- [Denial of Service Attack: Probe request flood, page A-7](#)
- [Denial of Service Attack: PS Poll Flood Attack, page A-6](#)
- [Denial of Service Attack: Re-association request flood, page A-8](#)
- [Denial of Service Attack: Unauthenticated Association, page A-7](#)

Denial of Service Attack: Association Flood

Alarm Description and Possible Causes

This DoS attack exhausts the access point's resources, particularly the client association table, by flooding the access point with a large number of spoofed client associations. At the 802.11 layer, shared-key authentication is flawed and rarely used. The other alternative is open authentication (null authentication) that relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker using such a vulnerability can emulate a large number of clients to flood a target access point's client association table by creating many clients. When the client association table overflows, legitimate clients cannot get associated; therefore, a DoS attack is committed (see [Figure 12-1](#)).

Figure 12-1 Association Flood



wIPS Solution

The wIPS detects spoofed MAC addresses and tracks the 802.1x actions and data communication after a successful client association to detect this form of DoS attack. After this attack is reported by the wIPS, you may log onto this access point to inspect its association table for the number of client associations.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing. For more information on MFP, see the *Cisco Wireless Control System Configuration Guide* or the NCS 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 a null authentication process. Association with these imitated clients follows the authentication process. These imitated clients do not, however, follow up with higher-level authentication, such as 802.1x or VPN, which leaves the protocol transaction half-finished. At this point, the attacked access point maintains a state in the client association table for each imitated client. When the access point'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 attack.

wIPS Solution

The wIPS tracks the client authentication process and identifies a DoS attack signature against an access point. Incomplete authentication and association transactions trigger the attack detection of the wIPS and statistical signature matching process.

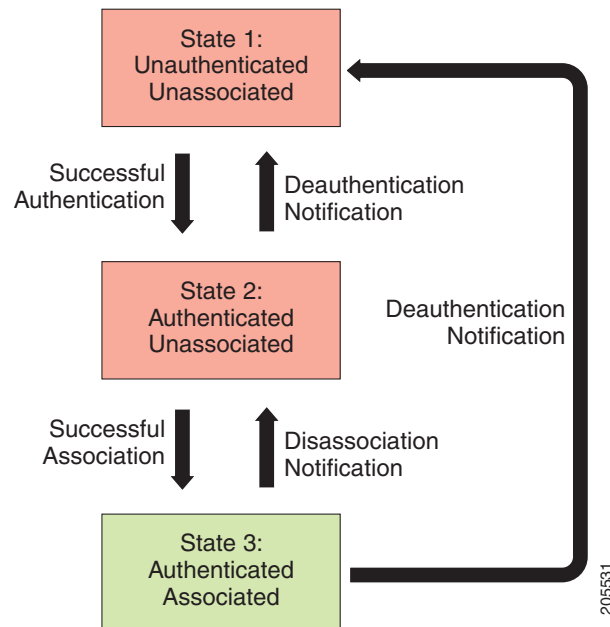
Denial of Service Attack: Authentication Flood

Attack tool: Void11

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement such a state machine according to the IEEE standard (see Figure 12-2). On the access point, each client 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.

Figure 12-2 Authentication Flood



A form of DoS 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 receipt of each individual authentication request, the target access point creates a client entry in State 1 of the association table. If open system authentication is used for the access point, the access point returns an *authentication success* frame and moves the client to State 2. If shared-key authentication is used for the access point, the access point sends an *authentication challenge* to the attacker'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 cannot authenticate and associate with this access point. This results in a DoS attack.

wIPS Solution

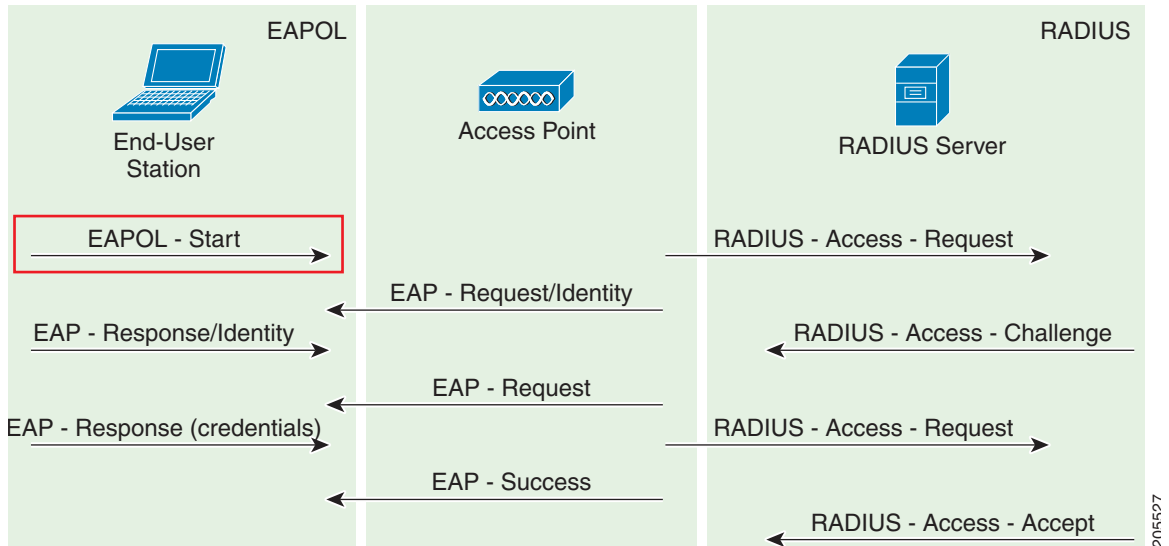
The wIPS detects this form of DoS attack by tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security analyst can log onto the access point to check the current association table status.

Denial of Service Attack: EAPOL-Start Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP over LANs (EAPOL). The 802.1x protocol starts with an EAPOL-Start frame sent by the client station to begin the authentication transaction. The access point responds to an EAPOL-start frame with an EAP identity request and some internal resource allocation (see Figure 12-3).

Figure 12-3 EAPOL-Start Protocol and EAPOL-Start Attack



An attacker attempts to disrupt an access point by flooding it with EAPOL-start frames to exhaust the access point internal resources.

wIPS Solution

The wIPS detects this form of DoS attack by tracking the 802.1x authentication state transition and particular attack signature.

Denial of Service Attack: PS Poll Flood 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 save mode for longer periods of time and to receive data from the access point only at specified intervals.

The wireless client device must inform the access point of the length of time that it is going to 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 spoofs 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 can be in the power safe mode and would miss the data frames.

wIPS Solution

The wIPS can detect this DoS attack that can cause the wireless client to lose legitimate data. Locate and remove the device from the wireless environment.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing. For more information on MFP, see the *Cisco Wireless Control System Configuration Guide* or the NCS online Help.

Denial of Service Attack: Unauthenticated Association

Alarm Description and Possible Causes

A form of DoS attack is to exhaust the access point's resources, particularly the client association table, by flooding the access point with a large number of spoofed client associations. At the 802.11 layer, shared-key authentication is flawed and rarely used. The other alternative is open authentication (null authentication) which relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker using such a vulnerability can imitate a large number of clients to flood a target access point's client association table by creating many clients. When the client association table overflows, legitimate clients cannot get associated causing a DoS attack.

wIPS Solution

The wIPS detects spoofed MAC addresses and tracks 802.1x actions and data communication after a successful client association to detect this form of DoS attack. After this attack is reported by the wIPS, you may log onto this access point to inspect its association table for the number of client associations.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing. For more information on MFP, see the *Cisco Wireless Control System Configuration Guide* or the NCS online Help.

Denial of Service Attack: Probe request flood

Alarm Description and Possible CAused

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

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 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, page A-12](#)
- [Denial of Service Attack: CTS Flood, page A-8](#)
- [Denial of Service Attack: MDK3-Destruction attack, page A-12](#)
- [Denial of Service Attack: RF Jamming Attack, page A-10](#)
- [Denial of Service Attack: RTS Flood, page A-11](#)
- [Denial of Service Attack: Queensland University of Technology Exploit, page A-9](#)
- [Denial of Service Attack: Virtual Carrier Attack, page A-11](#)

Denial of Service Attack: CTS Flood

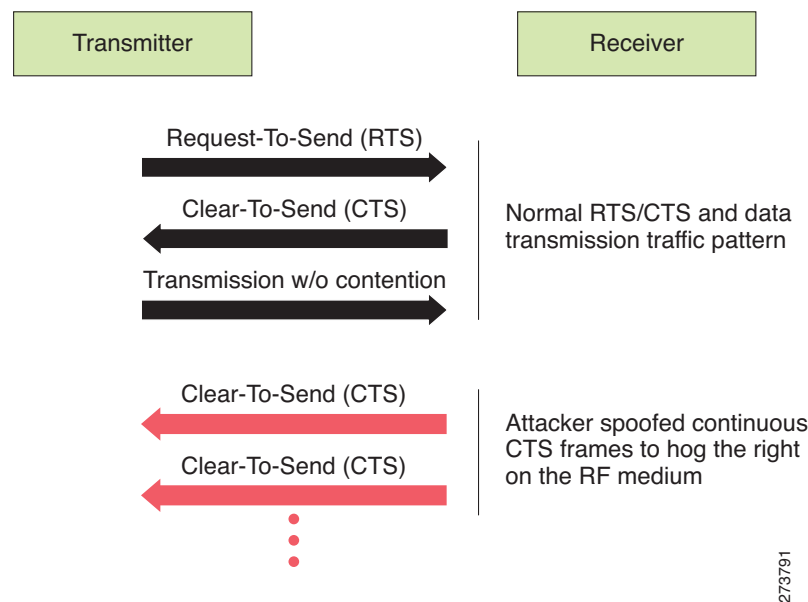
Attack tool: CTS Jack

Alarm Description and Possible Causes

As an optional feature, the IEEE 802.11 standard includes the RTS/CTS (request-to-send/clear-to-send) functionality to control the station access to the RF medium. The wireless device ready for transmission sends a RTS frame to acquire the right to the RF medium for a specified time duration. The receiver grants the right to the RF medium to the transmitter by sending a CTS frame of the same time duration. All wireless devices observing the CTS frame should yield the media to the transmitter for transmission without contention.

A wireless DoS attacker might 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 (see [Figure 12-4](#)).

Figure 12-4 CTS Spoof and Challenge to RF Control



wIPS Solution

The wIPS detects the abuse of CTS frames for a DoS attack.

Denial of Service Attack: Queensland University of Technology Exploit

Denial of Service Vulnerability in IEEE 802.11 Wireless Devices: US-CERT VU#106678 & Aus-CERT AA-2004.02

Alarm Description and Possible Causes

802.11 WLAN devices use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the basic access mechanism in which the WLAN device listens to the medium before starting any transmission and backs-off when it detects any existing transmission taking place. Collision avoidance combines the physical sensing mechanism and the virtual sense mechanism that includes the Network

Allocation Vector (NAV), the time before which the medium is available for transmission. Clear Channel Assessment (CCA) in the DSSS protocol determines whether a WLAN channel is clear so an 802.11b device can transmit on it.

Mark Looi, Christian Wullems, Kevin Tham and Jason Smith from the Information Security Research Centre, Queensland University of Technology, Brisbane, Australia, have recently discovered a flaw in the 802.11b protocol standard that may potentially make it vulnerable to DoS radio frequency jamming attacks.

This attack specifically attacks the CCA functionality. According to the AusCERT bulletin, "an attack against this vulnerability exploits the CCA function at the physical layer and causes all WLAN nodes within range, both clients and access points, to defer transmission of data for the duration of the attack. When under attack, the device behaves as if the channel is always busy, preventing the transmission of any data over the wireless network."

This DoS attack affects DSSS WLAN devices including IEEE 802.11, 802.11b, and low-speed (below 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, see the following:

- www.isrc.qut.edu.au
- <http://www.uscert.org.au/render.html?it=4091>
- <http://www.kb.cert.org/vuls/id/106678>

wIPS Solution

The wIPS detects this DoS attack and sets off the alarm. Locate and remove the responsible device from the wireless environment.

Denial of Service Attack: RF Jamming Attack

Alarm Description and Possible Causes

WLAN reliability and efficiency depend on the quality of the radio frequency (RF) media. Each RF is susceptible to RF noise impact. An attacker using this WLAN vulnerability can perform two types of DoS attacks:

- Disrupt WLAN service—At the 2.4-GHz unlicensed spectrum, the attack may be unintentional. A cordless phone, Bluetooth devices, microwave, wireless surveillance video camera, or baby monitor can all emit RF energy to disrupt WLAN service. Malicious attacks can manipulate the RF power at 2.4-GHz or 5-GHz spectrum with a high-gain directional antenna to amplify the attack impact from a distance. With free-space and indoor attenuation, a 1-kW jammer 300 feet away from a building can jam 50 to 100 feet into the office area. The same 1-kW jammer located inside a building can jam 180 feet into the office area. During the attack, WLAN devices in the target area are out of wireless service.
- Physically damage AP hardware—An attacker using a high-output transmitter with directional high gain antenna 30 yards away from an access point can pulse enough RF power to damage electronics in the access point putting it being permanently out of service. Such High Energy RF (HERF) guns are effective and are inexpensive to build.

wIPS Solution

The wIPS detects continuous RF noise over a certain threshold for a potential RF jamming attack.

Cisco Spectrum Intelligence also provides specific detection of non-802.11 jamming devices. For more information on Cisco Spectrum Intelligence, see the *Cisco Wireless Control System Configuration Guide* or the NCS online Help.

Denial of Service Attack: 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 wIPS 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 sub-frame 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 (such as association) 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 may 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 wIPS detects this DoS attack. Locate the device and take appropriate steps to remove it from the wireless environment.

Denial of Service Attack: Beacon 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: MDK3-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 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.

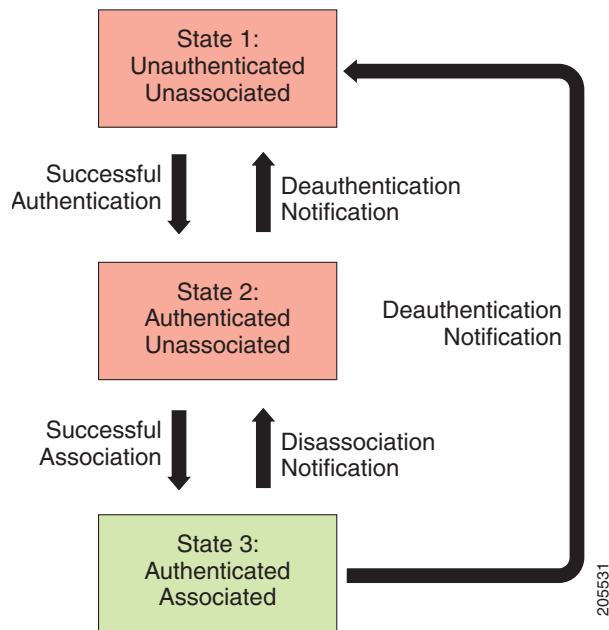
DoS attacks against client station include the following types:

- [“Denial of Service Attack: Authentication Failure Attack”](#) section on page A-13
- [“Denial of Service Attack: Block ACK flood”](#) section on page A-14
- [“Denial of Service Attack: De-Auth broadcast flood”](#) section on page A-15
- [“Denial of Service Attack: De-Auth flood”](#) section on page A-16
- [“Denial of Service Attack: EAPOL-Logoff Attack”](#) section on page A-19
- [“Denial of Service Attack: FATA Jack Tool Detected”](#) section on page A-20
- [“Denial of Service Attack: Premature EAP Failure”](#) section on page A-21
- [“Denial of Service Attack: Premature EAP Success”](#) section on page A-22
- [“Denial of Service Attack: Dis-Assoc Flood”](#) section on page A-18
- [“Denial of Service Attack: Probe response flood”](#) section on page A-22

Denial of Service Attack: Authentication Failure Attack

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this client state machine based on the IEEE standard (see [Figure 12-5](#)). A successfully associated client remains in State 3 in order to continue wireless communication. A client in State 1 and in State 2 cannot participate in the WLAN data communication process until it is authenticated and associated to State 3. IEEE 802.11 defines two authentication services: open system authentication and shared key authentication. Wireless clients go through one of these authentication processes to associate with an access point.

Figure 12-5 Authentication Failure Attack

A DoS attack spoofs invalid authentication request frames (with bad authentication service and status codes) being sent from an associated client in State 3 to an access point. Upon receipt of the invalid authentication requests, the access point updates the client to State 1, which disconnects wireless service of the client.

wIPS Solution

The wIPS 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 IEEE 802.11 authentication methods, such as open system and shared key. EAP and 802.1x based authentications are monitored by other alarms.

Denial of Service Attack: Block ACK 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 (ADDDBA) 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 ADDBA 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.

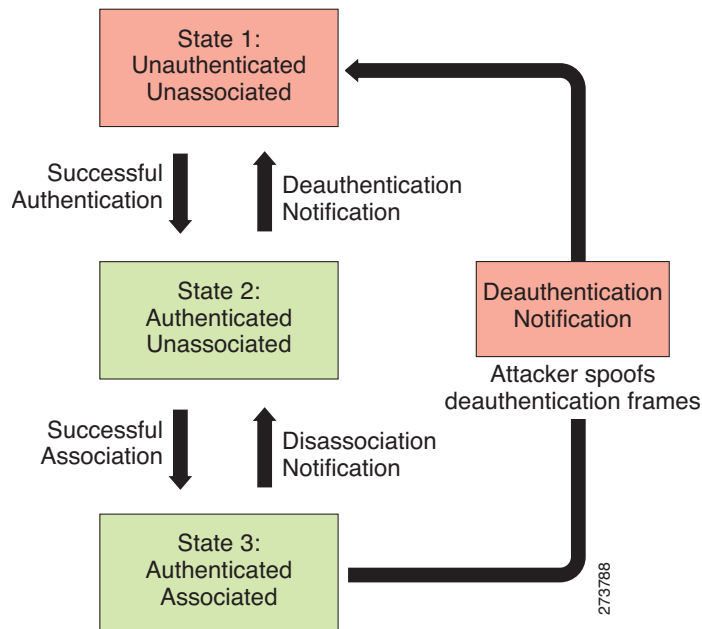
Denial of Service Attack: De-Auth broadcast flood

Attack tool: WLAN Jack, Void11, Hunter Killer

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client remains in State 3 to continue wireless communication. A client in State 1 and State 2 cannot participate in WLAN data communication until it is authenticated and associated to State 3 (see [Figure 12-6](#)).

Figure 12-6 Deauthentication Broadcast Attack



A form of DoS attack sends all clients of an access point to the unassociated or unauthenticated State 1 by spoofing deauthentication frames from the access point to the broadcast address. With current client adapter implementation, this form of attack is very effective and immediate in disrupting wireless services against multiple clients. Typically, client stations reassociate and reauthenticate to regain service until the attacker sends another deauthentication frame.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed 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 Wireless Control System Configuration Guide or the WCS online help.

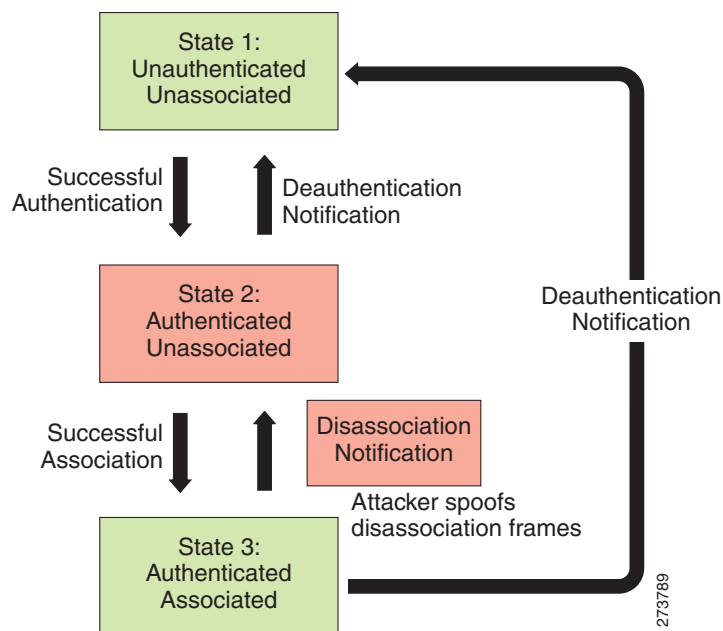
Denial of Service Attack: De-Auth flood

Attack tool: WLAN Jack, Void11

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client stays in State 3 in order to continue wireless communication. A client in State 1 and State 2 cannot participate in WLAN data communication until it is authenticated and associated to State 3 (see [Figure 12-7](#)).

Figure 12-7 Deauthentication Flood Attack



A form of DoS attack aims to send an access point's client to the unassociated or unauthenticated State 1 by spoofing deauthentication frames from the access point to the client unicast address. With current client adapter implementations, this form of attack is very effective and immediate for disrupting wireless services against the client. Typically, client stations reassociate and reauthenticate to regain service until the attacker sends another deauthentication frame. An attacker repeatedly spoofs the deauthentication frames to keep all clients out of service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed de-authentication frames and tracking client authentication and association states. When the alarm is triggered, the access point and client under attack are identified. The WLAN security officer can log 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 Wireless Control System Configuration Guide or the WCS online help.

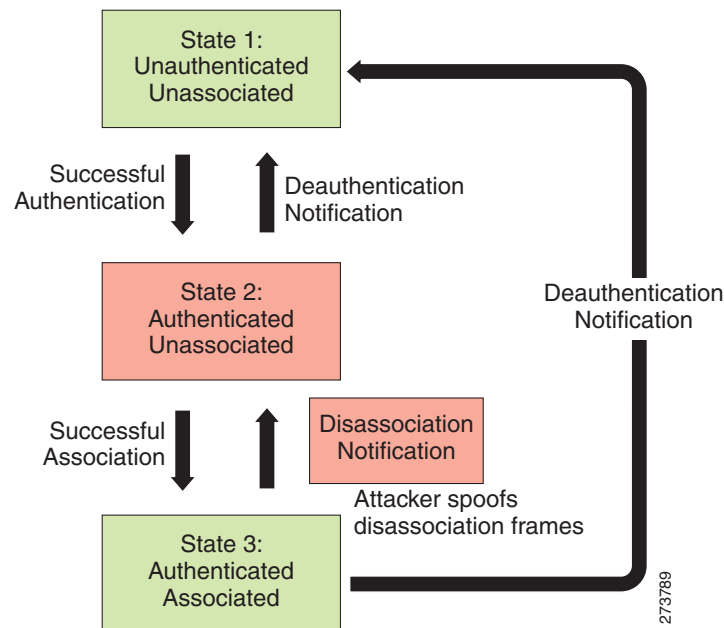
Denial of Service Attack: Dis-Association broadcast flood

Attack tool: ESSID Jack

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client station stays in State 3 in order to continue wireless communication. A client station in State 1 and State 2 cannot participate in WLAN data communication until it is authenticated and associated to State 3 (see [Figure 12-8](#)).

Figure 12-8 Disassociation Broadcast Attack



A form of DoS attack aims to send an access point's client to the unassociated or unauthenticated State 2 by spoofing disassociation frames from the access point to the broadcast address (all clients). With current client adapter implementations, this form of attack is effective and immediate for disrupting wireless services against multiple clients. Typically, client stations reassociate to regain service until the attacker sends another disassociation frame. An attacker repeatedly spoofs the disassociation frames to keep all clients out of service.

wIPS Solution

The wIPS detects this form of DoS attack by detecting spoofed disassociation frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log onto the access point to check the current association table status.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, see the *Cisco Wireless Control System Configuration Guide* or the NCS online Help.

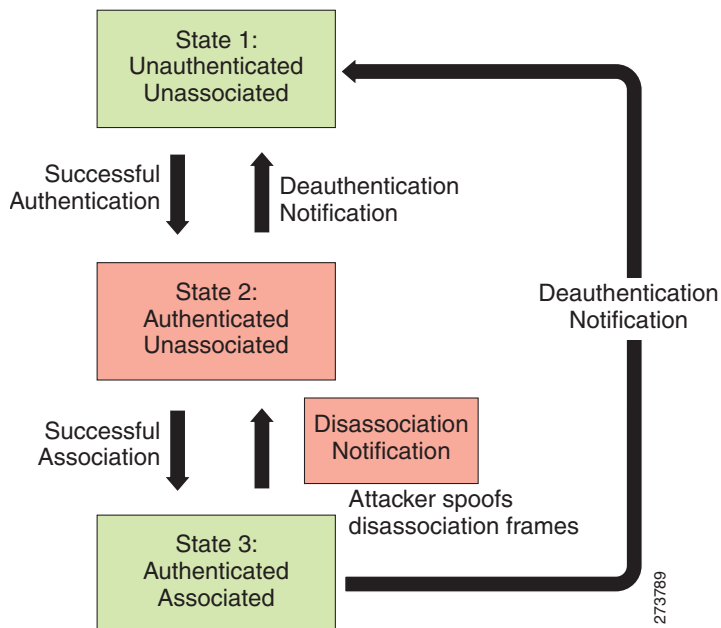
Denial of Service Attack: Dis-Assoc Flood

Attack tool: ESSID Jack

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client stays in State 3 in order to continue wireless communication. A client in State 1 and State 2 cannot participate in WLAN data communication until it is authenticated and associated to State 3 (see [Figure 12-9](#)).

Figure 12-9 Disassociation Flood Attack



A form of DoS attack aims to send an access point to the unassociated or unauthenticated State 2 by spoofing disassociation frames from the access point to a client. With client adapter implementations, this form of attack is effective and immediate for disrupting wireless services against this client. Typically, client stations reassociate to regain service until the attacker sends another disassociation frame. An attacker repeatedly spoofs the disassociation frames to keep the client out of service.

wIPS Solution

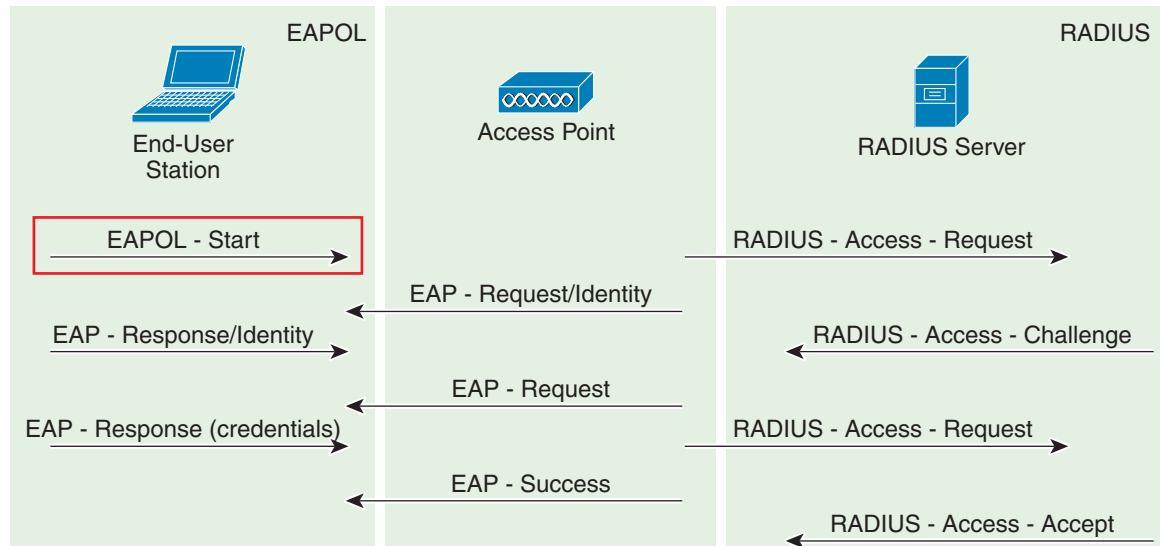
The wIPS detects this form of DoS attack by detecting spoofed disassociation frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log onto the access point to check the current association table status.

Denial of Service Attack: EAPOL-Logoff Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using Extensible Authentication Protocol (EAP) over LANs or EAPOL. The 802.1x protocol starts with a EAPOL-start frame to begin the authentication transaction. At the end of an authenticated session when a client station logs off, the client station sends an 802.1x EAPOL-logoff frame to terminate the session with the access point (see [Figure 12-10](#)).

Figure 12-10 EAPOL Logoff Attack



Because the EAPOL-logoff frame is not authenticated, an attacker can potentially spoof this frame and log the user off the access point, thus committing a DoS attack. The fact that the client is logged off from the access point is not obvious until it attempts communication through the WLAN. Typically, the disruption is discovered and the client reassociates 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

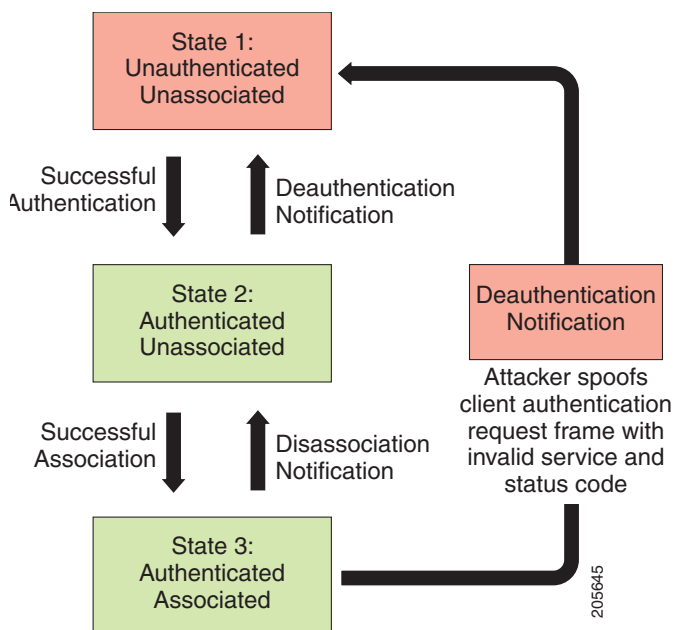
The wIPS detects this form of DoS attack by tracking 802.1x authentication states. When the alarm is triggered, the client and access point under attack are identified. The WLAN security officer logs onto the access point to check the current association table status.

Denial of Service Attack: FATA Jack Tool Detected

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this state machine based on the IEEE standard. A successfully associated client station stays in State 3 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 and shared key. Wireless clients go through one of these authentication processes to associate with an access point (see [Figure 12-11](#)).

Figure 12-11 Invalid Authentication Request Spoof



A form of DoS attack spoofs invalid authentication request frames (with bad authentication service and status codes) from an associated client in State 3 to an access point. Upon reception of the invalid authentication requests, the access point updates the client to State 1, which disconnects its wireless service.

FATA-jack is one of the commonly used tools to run a similar attack. It is a modified version of WLAN-jack and it sends authentication-failed packets along with the reason code of the previous authentication failure to the wireless station. This occurs after it spoofs the MAC address of the access point. FATA-jack closes most active connections and at times forces the user to reboot the station to continue normal activities.

wIPS Solution

The wIPS 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 wIPS 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). EAP and 802.1x based authentications are monitored by other alarms.

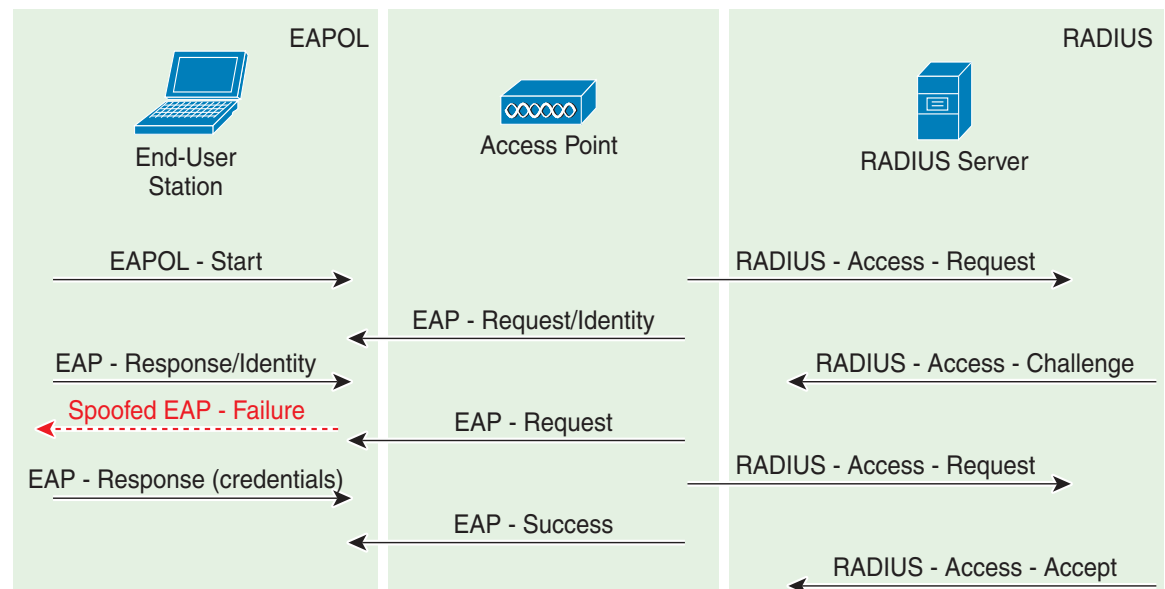
Cisco Management Frame Protection also provides complete proactive protection against frame and device spoofing. For more information on MFP, see the *Cisco Wireless Control System Configuration Guide* or the NCS online Help.

Denial of Service Attack: Premature EAP Failure

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using Extensible Authentication Protocol over LANs or EAPOL. The 802.1x protocol starts with an EAPOL-Start frame to begin the authentication transaction. When the 802.1x authentication packet exchange is complete with the back-end RADIUS server, the access point sends an EAP-success or EAP-failure frame to the client to indicate authentication success or failure (see [Figure 12-12](#)).

Figure 12-12 Premature EAP Failure Attack



The IEEE 802.1X specification prohibits a client from displaying its interface when the required mutual authentication is not complete. This enables a well-implemented 802.1x client station to avoid being fooled by a fake access point sending premature EAP-success packets.

An attacker keeps the client interface from appearing by continuously spoofing premature EAP-failure frames from the access point to the client to disrupt the authentication state on the client.

wIPS Solution

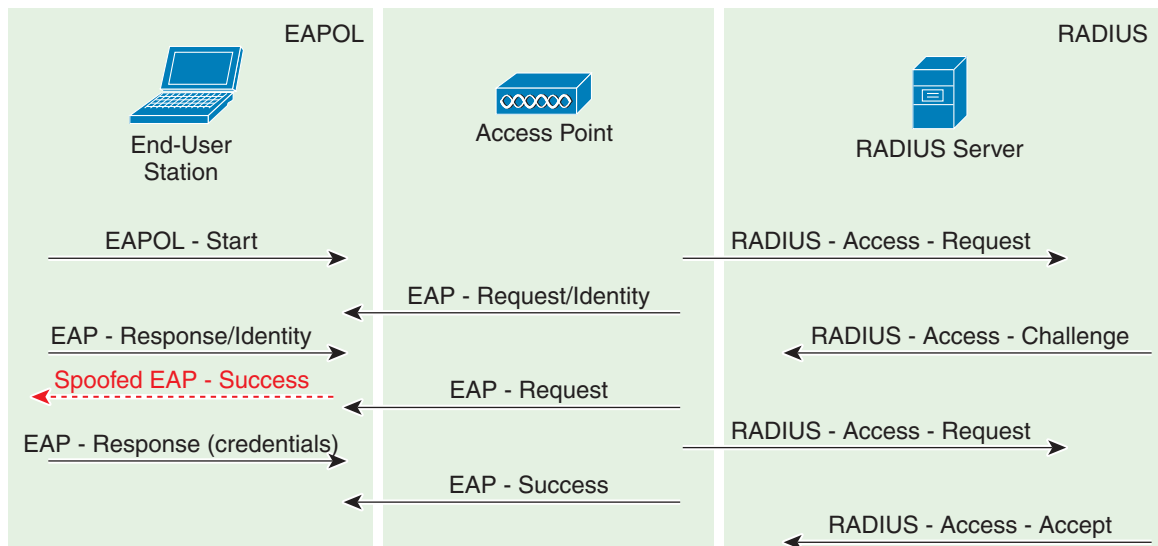
The wIPS detects this form of DoS attack by tracking the spoofed premature EAP-failure frames and the 802.1x authentication states for each client station and access point. Find the device and remove it from the wireless environment.

Denial of Service Attack: Premature EAP Success

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using Extensible Authentication Protocol over LANs or EAPOL. The 802.1x protocol starts with an EAPOL-start frame to begin the authentication transaction. When the 802.1x authentication packet exchange is completed with the back-end RADIUS server, the access point sends an EAP-success frame to the client to indicate a successful authentication (see Figure 12-13).

Figure 12-13 EAP Success Attack



The IEEE 802.1X specification prohibits a client from displaying its interface when the required mutual authentication has not been completed. This enables a well-implemented 802.1x client station to avoid being fooled by a fake access point sending premature EAP-success packets to bypass the mutual authentication process.

An attacker keeps the client interface from appearing by continuously spoofing premature EAP-success frames from the access point to the client to disrupt the authentication state.

wIPS Solution

The wIPS detects this form of DoS attack by tracking spoofed premature EAP-success frames and the 802.1x authentication states for each client station and access point. Find the device and remove it from the wireless environment.

Denial of Service Attack: Probe response flood

Alarm Description and Possible Causes

A form of Denial of Service attack allows the attacker to prevent a station from associating to a valid corporate AP. In a typical wireless transaction, when a station wishes to associate to an AP, it transmits a probe request from to obtain information about the AP's network. The station will then wait for the resulting probe response frame from the AP. An attacker can take advantage of this process by flooding

the environment with invalid probe responses, thus preventing the station from receiving the response from the valid AP. As a result, the station is rendered unable to connect to the wireless network, and a denial of service attack is initiated.

wIPS Solution

The wIPS server monitors the levels of probe response frames detected and will trigger a Probe Request Flood alarm when the threshold is exceeded. Even in cases where the responses 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.

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 an unsuspecting 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, page A-24](#)
- [AirPwn, page A-25](#)
- [Airsnarf Attack, page A-26](#)
- [Bad EAP-TLS frames, page A-27](#)
- [Brute Force Hidden SSID, page A-28](#)
- [Chopchop Attack, page A-27](#)
- [Day-Zero Attack by WLAN SecurityAnomaly, page A-28](#)
- [Day-Zero Attack by Device Security Anomaly, page A-30](#)
- [Device Broadcasting XSS SSID, page A-31](#)
- [Device Transmitting Reserved MGMT/CTRL Frames, page A-32](#)
- [Device Probing for APs, page A-32](#)
- [Dictionary Attack on EAP Methods, page A-33](#)
- [EAP Attack Against 802.1x Authentication, page A-34](#)
- [Fake APs Detected, page A-34](#)
- [Fake DHCP Server Detected, page A-35](#)
- [Fast WEP Crack tool Detected, page A-36](#)
- [Fragmentation Attack, page A-36](#)

- [HoneyPot AP detected, page A-37](#)
- [Hot-Spotter Tool Detected, page A-38](#)
- [Identical Send and Receive Address, page A-39](#)
- [Improper Broadcast Frames, page A-39](#)
- [Karma tool Detected, page A-39](#)
- [Malformed 802.11 Packets Detected, page A-40](#)
- [Man-in-the-Middle Attack Detected, page A-40](#)
- [NetStumbler Detected, page A-41](#)
- [NetStumbler Victim Detected, page A-42](#)
- [PSPF Violation detected, page A-43](#)
- [Sky Jack Attack Detected, page A-44](#)
- [Soft AP or Host AP Detected, page A-46](#)
- [Spoofed MAC Address Detected, page A-46](#)
- [Suspicious After-Hours Traffic Detected, page A-47](#)
- [Unauthorized Association by Vendor List, page A-47](#)
- [Unauthorized Association Detected, page A-48](#)
- [Wellenreiter Detected, page A-48](#)
- [WiFiTap Tool Detected, page A-49](#)
- [Potential ASLEAP Attack Detected, page A-44](#)
- [Potential HoneyPot AP Detected, page A-46](#)

ASLEAP tool detected

Alarm Description and Possible Causes

WLAN devices using static WEP key for encryption are vulnerable to the WEP key cracking attack (See Weaknesses in the Key Scheduling Algorithm of RC4-I by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information).

Cisco Systems introduced LEAP (Lightweight Extensible Authentication Protocol) to leverage the existing 802.1x framework to avoid such WEP key attacks. The Cisco LEAP solution provides mutual authentication, dynamic per session and per user keys, and configurable WEP session key time out. The LEAP solution was considered a stable security solution and is easy to configure.

There are hacking tools that compromise wireless LAN networks running LEAP by using off-line dictionary attacks to break LEAP passwords. After detecting WLAN networks that use LEAP, this tool de-authenticates users which forces them to reconnect and provide their 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.

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

Alarm Description and Possible Causes

A hotspot is any location where Wi-Fi network access is made available for the general public. Hotspots are found in airports, hotels, coffee shops, and other places where business people tend to congregate. They are important network access services for business travelers.

Customers are able to connect to the legitimate access point and receive service using a wireless-enabled laptop or handheld. Most hotspots do not require the user to have any advanced authentication mechanism to connect to the access point other than popping up a web page for the user to log in. The criterion for entry is dependent only on whether or not the subscriber has paid the subscription fees. In a wireless hotspot environment, no one should be trusted. Due to current security concerns, some WLAN hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user.

The four components of a basic hotspot network include:

- Hotspot Subscribers—Valid users with a wireless-enabled laptop or handheld and valid log in for accessing the hotspot network.
- WLAN Access Points—Can be small office home office (SOHO) gateways or enterprise-level access points depending upon the hotspot implementation.
- Hotspot Controllers—Deals with user authentication, gathering billing information, tracking usage time, filtering functions and so on. This can be an independent machine or incorporated in the access point itself.
- Authentication Server—Contains the log in credentials for the subscribers. Most hotspot controllers verify subscribers' credentials with the authentication server.

Airsnarf is a wireless access point setup utility that shows how a hacker can steal username and password credentials from public wireless hotspots.

Airsnarf, a shell script-based tool, creates a hotspot complete with a captive portal where the users enter their log in information. Important values such as local network information, gateway IP address, and SSID can be configured within the airsnarf configuration file. This tool initially broadcasts a very strong signal that disassociates the hotspot wireless clients from the authorized access point connected to the Internet. The wireless clients assume that they are temporarily disconnected from the Internet due to some unknown issue and they try to log in again. Wireless clients that associate to the Airsnarf access point receive the IP address, DNS address, and gateway IP address from the rogue Airsnarf access point instead of the legitimate access point installed by the hotspot operator. A web page requests a username and password and the DNS queries are resolved by the rogue Airsnarf access point. The username and password entered are collected by the hacker.

The username and password can be used in any other hotspot location of the same provider anywhere in the nation without the user realizing the misuse. The only case where it can have lesser impact is if the hotspot user is connected using a pay-per-minute usage scheme.

The Aircsnarf tool can also penetrate the laptop clients that are unknowingly connected to the Aircsnarf access point. The Aircsnarf tool can be downloaded by hackers from <http://aircsnarf.shmoo.com/>.

wIPS Solution

The wIPS detects the wireless device running the Aircsnarf tool. Appropriate action must be taken by the administrator to remove the Aircsnarf 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.

Chopchop Attack

Alarm Description and Possible Causes

It is well publicized that a WLAN device using a static WEP key for encryption is vulnerable to various WEP cracking attacks. See the *Weaknesses in the Key Scheduling Algorithm of RC4 - I* by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information.

A cracked WEP secret key offers no encryption protection for data to be transmitted, leading to compromised data privacy. The WEP key, which is in most cases 64-bit or 128-bit (some vendors also offer 152-bit encryption), is a secret key specified by the user, linked with the 24-bit IV (Initialization Vector). The chopchop tool was written for the Linux operating system by Korek to exploit a weakness in WEP and decrypt the WEP data packet. However, the chopchop tool only reveals the plaintext. The attacker uses the packet capture file of a previously injected packet during the initial phase and decrypts the packet by retransmitting modified packets to the attacked network. When the attack is completed, the chopchop tool produces an unencrypted packet capture file and another file with Pseudo Random Generation Algorithm (PRGA) information determined during the decryption process. The PRGA is then XORed with the cyphertext to obtain the plaintext.

The following example commands indicate a chopchop attack:

```
aireplay-ng -4 -h XX:XX:XX:XX:XX:XX -b YY:YY:YY:YY:YY:YY ath0
```

where

- 4: Indicates a chopchop attack
- h XX:XX:XX:XX:XX:XX: Identifies a MAC address of an associated client
- b YY:YY:YY:YY:YY:YY: Identifies the MAC address of the access point

ath0: Identifies the wireless interface name

Access points that drop data packets shorter than 60 bytes may not be vulnerable to this kind of attack. If an access point drops packets shorter than 42 bytes, aireplay tries to guess the rest of the missing data, as far as the headers are predictable. If an IP packet is captured, it additionally checks if the checksum of the header is correct after guessing the missing parts of it. This attack requires at least one WEP data packet. A chopchop attack also works against dynamic WEP configurations. The wIPS is able to detect potential attacks using the chopchop tool.

wIPS Solution

The wIPS activates an alert when a potential chopchop attack is in progress. WEP should not be used in the corporate environment and appropriate measures should be taken to avoid any security holes in the network and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard.

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.

Day-Zero Attack by WLAN SecurityAnomaly

Alarm Description and Possible Causes

WLAN performance efficiency is constantly challenged by the dynamics of the RF environment and the mobility of client devices. A closely monitored and well tuned WLAN system can achieve a higher throughput than a poorly managed one. Radio Resource Management (RRM) built into the Cisco Unified Wireless Network monitors and dynamically corrects performance issues found in the RF environment. Further performance anomaly monitoring may be done through the Wireless IPS system. For more information on RRM, see the NCS online Help.

The 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. Performance alarms are generated and classified in the following categories in the event of any performance degradation:

- RF Management—The wIPS monitors the physical RF environment that is dynamic and very often the source of WLAN performance problems. While monitoring on the RF environment, the server characterizes the following WLAN fundamentals and reports problems accordingly:
 - Channel interference and channel allocation problems
 - Channel noise and non-802.11 signals
 - WLAN RF service under-coverage area
 - Classic RF hidden-node syndrome
- Problematic traffic pattern—Many WLAN performance problems including the RF multi-path problem manifest themselves in the MAC layer protocol transactions and statistics. By tracking and analyzing the wireless traffic, the wIPS is able to spot performance inefficiencies and degradations early on. In many cases, the wIPS can determine the cause of the detected performance problem and suggest counter measures. The wIPS tracks MAC layer protocol characteristics including the following:
 - Frame CRC error
 - Frame retransmission
 - Frame speed (1, 2, 5.5, 11, ... Mbps) usage and distribution
 - Layer 2 frame fragmentation
 - Access point and station association, reassociation and disassociation relationship
 - Roaming hand-off
- Channel or device overloaded—The wIPS monitors and tracks the load to ensure smooth operation with both channel bandwidth limitation or the WLAN device resource capacity. In the event of unsatisfactory performance by the WLAN due to under-provisioning or over-growth, the wIPS raises alarms and offers specific details. RF has no boundaries that can lead to your WLAN channel utilization to increase significantly even when your neighbor installs new WLAN devices in an adjoining channel. The wIPS monitors your WLAN to ensure proper bandwidth and resource provisioning.
- Deployment and operation error—The wIPS scans the airwaves for configuration and operation errors. The following specific areas are continuously monitored:
 - Inconsistent configuration among access points servicing the same SSID
 - Configuration against the principles of best practice
 - Connection problems caused by client/access point mismatch configuration
 - WLAN infrastructure device down or reset
 - Flaws in WLAN device implementation
- IEEE 802.11e and VoWLAN issues—The IEEE 802.11e standard adds quality of service (QoS) features and multimedia support to the existing 802.11 a/b/g wireless standard. This is done while maintaining full backward compatibility with these standards. The QoS feature is critical to voice and video applications. Wireless LAN has limited bandwidth and high overheads as compared to the traditional wired Ethernet. The throughput is reduced for a variety of reasons including the RTS/CTS mechanism, packet fragmentation, packet retransmission, acknowledgements, and collisions.

WIPS Solution

The WIPS has detected a single Performance Intrusion policy violation on a large number of devices in the wireless network. Either the number of devices violating the specific policy in the time period specified are observed or there is a sudden percentage increase in the number of devices as specified in the threshold settings for the alarm. Depending on the Performance Intrusion violation, it is suggested that the devices be monitored and located to carry out further analysis.

For example:

- If the AP overloaded by stations alarm is generated by a large number of devices, it may indicate that a hacker has generated thousands of stations and forcing them to associate to the corporate access point. If this occurs, legitimate corporate clients cannot connect to the access point.
- Excessive frame retries on the wireless devices may indicate such things as noise, interference, packet collisions, multi-path, and hidden node syndrome.

Day-Zero Attack by Device Security Anomaly

Alarm Description and Possible Causes

The addition of WLANs in the corporate environment introduces a whole new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk of outside penetration and attack. Besides rogue access points, there are many other wireless security vulnerabilities which compromise the wireless network such as misconfigured and unconfigured access points. There can also be DoS (denial of service) attacks from various sources against the corporate network.

NCS provides automated security vulnerability assessment within the wireless infrastructure that proactively reports any security vulnerabilities or mis-configurations. Further assessment may be done over-the-air through the Wireless IPS system. 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 (Static WEP encryption, VPN, Fortress, Cranite, 802.11i and 802.1x)—Common security violations in this category (authentication and encryption) include mis-configurations, out-of-date software or firmware, and suboptimal choice of corporate security policy.
- Rogue, monitored, and ad-hoc mode devices—Rogue devices must be detected and removed immediately in order to protect the integrity of the wireless and wired enterprise network.
- Configuration vulnerabilities—Implementing a strong deployment policy is fundamental to a secure WLAN. However, enforcing the policy requires constant monitoring to catch violations caused by mis-configuration or equipment vendor implementation errors. With the increased trend on laptops with built-in Wi-Fi capabilities, the complexity of WLAN configuration extends beyond access points to the user laptops. WLAN device configuration management products can make the configuration process easier, but the need for validation persists especially in laptops with built-in but unused and unconfigured Wi-Fi.
- Intrusion detection on security penetration—A form of wireless intrusion includes breaching the WLAN authentication mechanism in order to gain access to the wired network or the wireless devices. A Dictionary attack on the authentication method is a very common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked AP attack on a unsuspecting wireless client may fool the client

into associating with a fake access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.

- Intrusion detection on denial of service attacks—Wireless DoS (denial of service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLAN at layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example, RF jamming attack with high power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

wIPS Solution

The wIPS has detected a single Security IDS/IPS policy violation on a large number of devices in the wireless network. Either the number of devices violating the specific policy in the time period specified are observed or there is a sudden percentage increase in the number of devices as specified in the threshold settings for the alarm. Depending on the Security IDS/IPS violation, it is suggested that the devices are monitored and located to carry out further analysis to verify if they are compromising the Enterprise wireless network in any way (attack or vulnerability). If this is an increase in the number of rogue devices, it may indicate an attack against the network. The WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find it.

If there is a sudden increase in the number of client devices with encryption disabled, it may be necessary to revisit the Corporate Security Policy and enforce users to use the highest level of encryption and authentication according to the policy rules.

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 Transmitting Reserved MGMT/CTRL Frames

Alarm Description and Possible Causes

wIPS Solution

Device Probing for APs

Some commonly used scan tools include: NetStumbler (newer versions), MiniStumbler (newer versions), MACStumbler, WaveStumbler, PrismStumbler, dStumbler, iStumbler, Aerosol, Boingo Scans, WiNc, AP Hopper, NetChaser, Microsoft Windows XP scans.

Alarm Description and Possible Causes

The wIPS detects wireless devices probing the WLAN and attempting association (such as association request for an access point with any SSID).

Such devices can 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 (see [Figure 12-14](#)).

Figure 12-14 War Chalker Universal Symbols

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid X bandwidth
CLOSED NODE	ssid O
WEP NODE	ssid access contact W bandwidth

blackbeltjones.com/warchalking 2006048

- War-walking—War-walking is similar to war-driving, but the hacker is on foot instead of a car.
- War-flying—War-flying refers to sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet relay chat sessions from an altitude of 1,500 feet on a war-flying trip.

Legitimate Wireless Client Attempting Risky Association

The second potential security threat for this alarm may be more damaging. Some of these alarms can be from legitimate and authorized wireless clients on your WLAN who are attempting to associate with any available access point including your neighbor's access point or the more damage-causing rogue access point. This potential security threat can be from a Microsoft Windows XP laptop with a built-in Wi-Fi card or laptops using wireless connectivity tools such as the Boingo client utility and the WiNc client utility. When associated, this client station can be accessed by an intruder leading to a major security breach. Even worse, the client station may bridge the unintended access point with your company's wired LAN. Typically, laptops are equipped with built-in Wi-Fi cards and, at the same, are physically attached to your company WLAN for network connectivity. Your wired network is exposed if the Windows bridging service is enabled on that Windows laptop. To be secure, configure all client stations with specific SSIDs to avoid associating with an unintended access point. Also consider mutual authentication such as 802.1x and various EAP methods.

The wIPS also detects a wireless client station probing the WLAN for an anonymous association such as an association request for an access point with any SSID) using the NetStumbler tool. The device probing for access point alarm is generated when hackers use the latest versions of the NetStumbler tool. For older versions, the NetStumbler detected alarm is triggered.

NetStumbler is the most widely used tool for war-driving and war-chalking. The website of NetStumbler offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or more recent operating systems. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to search shopping malls and retail stores.

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure the access points to not broadcast SSIDs. Use the wIPS to determine 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 framework for wired or wireless LAN authentication. An EAP framework allows flexible authentication protocol implementation. Some implementations of 802.1x or WPA use authentication protocols such as LEAP, MD5, OTP (one-time-password), TLS, and TTLS. Some of these authentication protocols are based on the username and password mechanism in which the username is transmitted without encryption and the password is used to answer authentication challenges.

Most password-based authentication algorithms are susceptible to dictionary attacks. During a dictionary attack, an attacker gains the username from the unencrypted 802.1x identifier protocol exchange. The attacker then tries to guess a user'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 a password being a common word, name, or combination of both with a minor modification such as a trailing digit or two.

A dictionary attack can take place actively online, where an attacker repeatedly tries all the possible password combinations. Online dictionary attacks can be prevented using lock-out mechanisms available on the authentication server (RADIUS servers) to lock out the user after a certain number of invalid log in attempts. A dictionary attack can also take place offline, where an attacker captures a successful authentication challenge protocol exchange and then tries to match the challenge response

with all possible password combinations. Unlike online attacks, offline attacks are not easily detected. Using a strong password policy and periodically expiring user passwords significantly reduces an offline attack tool's success.

wIPS Solution

The wIPS detects online dictionary attacks by tracking 802.1x authentication protocol exchange and the user identifier usages. When a dictionary attack is detected, the alarm message identifies the username and attacking station's MAC address.

The wIPS advises switching username and password based authentication methods to encrypted tunnel based authentication methods such as PEAP and EAP-FAST, which are supported by many vendors including Cisco.

EAP Attack Against 802.1x Authentication

Alarm Description and Possible Causes

IEEE 802.1x provides an Extensible Authentication Protocol (EAP) framework for wired or wireless LAN authentication. An EAP framework allows flexible authentication protocol implementation. Some implementations of 802.1x or WPA use authentication protocols such as LEAP, MD5, OTP (one-time-password), TLS, TTLS, and EAP-FAST. Some of these authentication protocols are based on the username and password mechanism, where the username is transmitted clear without encryption and the password is used to answer authentication challenges.

Most password-based authentication algorithms are susceptible to dictionary attacks. During a dictionary attack, an attacker gains the username from the unencrypted 802.1x identifier protocol exchange. The attacker attempts to guess a user's password and gain network access by using every "word" in a dictionary of common passwords or possible combinations of passwords. A dictionary attack relies on the fact that a password is often a common word, name, or combination of words or names with a minor modification such as a trailing digit or two.

Intruders with the legitimate 802.1x user identity and password combination (or valid certificate) can penetrate the 802.1x authentication process without the proper knowledge of the exact EAP-type. The intruder tries different EAP-types such as TLS, TTLS, LEAP, EAP-FAST, or PEAP to successfully log onto the network. This is a trial and error effort because there are only a handful of EAP-types for the intruder to try and manage to get authenticated to the network.

wIPS Solution

The wIPS detects an attempt by an intruder to gain access to the network using different 802.1x authentication types. Take appropriate steps to locate the device and remove it from the wireless environment.

Fake APs Detected

Alarm Description and Possible Causes

The Fake AP tool is meant to protect your WLAN acting as a decoy to confuse war-drivers using NetStumbler, Wellenreiter, MiniStumbler, Kismet, and so on. The tool generates beacon frames imitating thousands of counterfeit 802.11b access points. War-drivers encountering a large number of access points cannot identify the real access points deployed by the user. This tool, although very

effective in fending off war-drivers, poses other disadvantages such as bandwidth consumption, misleading legitimate client stations, and interference with the WLAN management tools. Running the Fake AP tool in your WLAN is not recommended.

wIPS Solution

The administrator should locate the device running the Fake AP tool and remove it from the wireless environment.

Fake DHCP Server Detected

Alarm Description and Possible Causes

Dynamic Host Configuration Protocol (DHCP) is used for assigning dynamic IP addresses to devices on a network.

DHCP address assignment takes place as follows:

-
- Step 1** The client NIC sends out a DHCP discover packet, indicating that it requires a IP address from a DHCP server.
 - Step 2** The server sends a DHCP offer packet with the IP address.
 - Step 3** The client NIC sends a DHCP request, informing the DHCP server that it wants to be assigned the IP address sent by the servers offer.
 - Step 4** The server returns a DHCP ACK, acknowledging that the NIC has sent a request for a specific IP address.
 - Step 5** The client's interface assigns or binds the initially offered IP address from the DHCP server.

The DHCP server should be a dedicated machine and part of the enterprise wired network or it can be a wireless/wired gateway. Other wireless devices can have the DHCP service running innocently or maliciously so as to disrupt the WLAN IP service. Wireless clients that are requesting an IP address from the DHCP server may then connect to these fake DHCP servers to get their IP address because the clients do not have any means to authenticate the server. These fake DHCP servers may give the clients non-functional network configurations or divert all the client's traffic through them. The hackers can then eavesdrop on every packet sent by the client. With the aid of rogue DNS servers, the hacker can also send the users to fake web page log ins to get username and password credentials. It can also give out non-functional and non-routable IP addresses to achieve a DoS attack. This sort of attack is generally against a WLAN without encryption such as hotspots or trade show networks.

wIPS Solution

The wIPS detects such wireless STAs running the DHCP service and providing IP addresses to unaware users.

When the client is identified and reported, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the device.

Fast WEP Crack tool Detected

Alarm Description and Possible Causes

It is well publicized that WLAN devices using static WEP key for encryption are vulnerable to WEP key cracking attack (See *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 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 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.

NCS also provides automated security vulnerability scanning that proactively reports any access points configured to utilize weak encryption or authentication. For more information on automated security vulnerability scanning, see the NCS online Help.

Fragmentation Attack

Alarm Description and Possible Causes

It is well publicized that a WLAN device using a static WEP key for encryption is vulnerable to various WEP cracking attacks. See *Weaknesses in the Key Scheduling Algorithm of RC4 - I* by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information.

A cracked WEP secret key offers no encryption protection for data to be transmitted which leads to compromised data privacy. The WEP key, which is in most cases 64-bit or 128-bit (few vendors also offer 152-bit encryption), is the secret key specified by the user and linked with the 24-bit IV (Initialization Vector).

According to <http://www.aircrack-ng.org/doku.php?id=fragmentation&s=fragmentation>, the aircrack program obtains a small amount of keying material from the packet and then attempts to send ARP and/or LLC packets with known information to an access point. If the packet gets successfully echoed back by the access point, then a larger amount of keying information can be obtained from the returned packet. This cycle is repeated several times until 1500 bytes (less in some cases) of PRGA are obtained.

This attack does not recover the WEP key itself, but merely obtains the PRGA. The PRGA can then be used to generate packets with packetforge-ng which can be used for various injection attacks.

The following example commands indicate a fragmentation attack:

```
aireplay-ng -5 -h XX:XX:XX:XX:XX:XX -b YY:YY:YY:YY:YY:YY ath0
```

where

5: Indicates a fragmentation attack

-h XX:XX:XX:XX:XX:XX: Identifies a MAC address of an associated client

-b YY:YY:YY:YY:YY:YY: Identifies the MAC address of the access point

ath0: Identifies the wireless interface name

wIPS Solution

The wIPS detects potential fragmentation attacks in progress against the Wi-Fi network. Further, wIPS 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 of Service

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.

wIPS Solution

Although this degradation of service doesn't necessarily indicate a wireless attack, the reduction in transmit speed can have a negative affect on network performance. As such, users should identify and eliminate the legacy device in order to maintain an optimal 802.11n deployment.

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

Alarm Description and Possible Causes

A hotspot is any location where Wi-Fi network access is 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 services 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

When the rogue access point is identified and reported by the wIPS, 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 Cause

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.

wIPS Solution

An Improper Broadcast Frames alarm is indicative of a potential attack which, if left unchecked, could impede network performance. Steps should be taken to locate the source of the invalid frames and eliminate it from the wireless environment as soon as possible.

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.

Malformed 802.11 Packets Detected

Alarm Description and Possible Causes

Hackers using illegal packets (malformed non-standard 802.11 frames) can force wireless devices to behave in an unusual manner. Illegal packets can cause the firmware of a few vendor's wireless NICs to crash.

Examples of such vulnerability includes NULL probe response frame (null SSID in the probe response frame) and oversized information elements in the management frames. These ill-formed frames can be broadcasted to cause multiple wireless clients to crash.

wIPS Solution

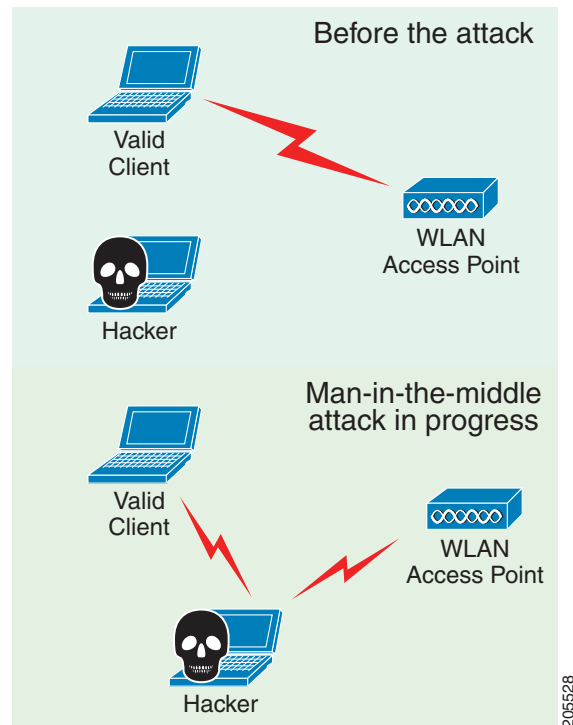
The wIPS can detect these illegal packets that may cause some NICs to lock up and crash. Also, wireless clients experiencing blue page or lock-up problem during the attack period should consider upgrading the WLAN NIC driver or the firmware.

When the client is identified and reported by the wIPS, the WLAN administrator may use the device locator to locate it.

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 (see [Figure 12-15](#)).

Figure 12-15 Man-in-the-Middle Attack

A common MITM attack involves the hacker sending spoofed disassociation or deauthentication frames. The hacker station then spoofs the MAC address of the client to continue an association with the access point. At the same time, the hacker sets up a spoofed access point in another channel to keep the client associated. All traffic between the valid client and access point then passes through the hacker's station.

One of the most commonly used MITM attack tools is Monkey-Jack.

wIPS Solution

The wIPS recommends the use of strong encryption and authentication mechanisms to thwart any MITM attacks by hackers. One way to avoid such an attack is to prevent MAC address spoofing by using MAC address exclusion lists and monitoring the RF channel environment.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MITM attacks. For more information on MFP, see the *Cisco Wireless Control System Configuration Guide* or the NCS online Help.

NetStumbler Detected

Alarm Description and Possible Causes

The wIPS 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 wIPS generates the *NetStumbler detected* alarm (see [Figure 12-16](#)).

Figure 12-16 War-Chalker Universal Symbols

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid X bandwidth
CLOSED NODE	ssid O
WEP NODE	ssid access contact W bandwidth
blackbeltjones.com/warchalking	

2006048

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) 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. The website of NetStumbler offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or later versions. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas.

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 wIPS to see which of your access points is broadcasting an SSID in the beacons.

NCS also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, see the NCS online Help.

NetStumbler Victim Detected

Alarm Description and Possible Causes

The wIPS detects a wireless client station probing the WLAN for an anonymous association (such as association request for an access point with any SSID) using the NetStumbler tool. The Device probing for access point alarm is generated when hackers more recent versions of the NetStumbler tool. For older versions, the wIPS 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) 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 website of NetStumbler 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.

wIPS Solution

The wIPS alerts the user when it observes that a station running Netstumbler is associated to a corporate access point. 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 wIPS to see which access point is broadcasting its SSID in the beacons.

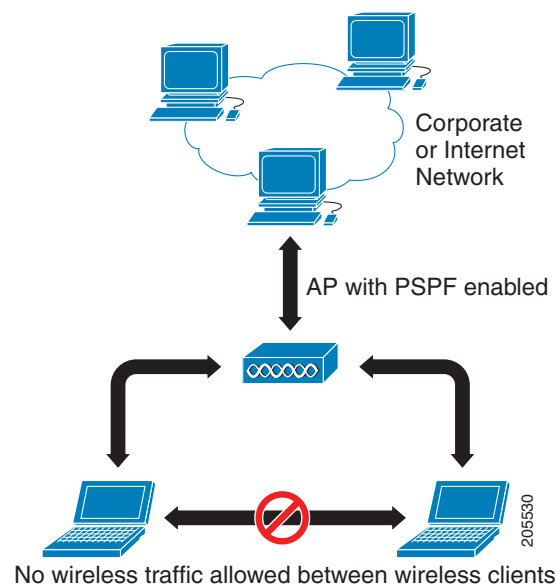
PSPF Violation detected

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 (see [Figure 12-17](#)).

Figure 12-17 PSPF Enabled On The Network



wIPS Solution

The wIPS detects PSPF violations. If a wireless client attempts to communicate with another wireless client, the wIPS 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.

Sky Jack Attack Detected

Alarm Detected and Possible Causes

wIPS Solution

Soft AP or host AP detected

Alarm Description and Possible Causes

A host-based access point (desktop or a laptop computer serving as a wireless access point) represents two potential threats to enterprise security. First, host based access points are not typically part of the enterprise wireless infrastructure and are likely to be rogue devices which do not conform to the corporate security policy. Second, host-based access points are used by wireless attackers as a convenient platform to implement various known intrusions such as man-in-the-middle, honey-pot access point, access point impersonation, and DoS (denial-of-service) attacks. Since software tools for turning a desktop or laptop into an access point can be easily downloaded from the Internet, host-based access points are more than just a theoretical threat.

Some laptops are shipped with the HostAP software pre-loaded and activated. Once the laptops connect to the enterprise wireless network, they expose the wireless network to the hackers.

wIPS Solution

The Cisco Adaptive Wireless IPS's detected soft access point should be treated as a rogue access point as well as a potential intrusion attempt. Once the soft access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

Potential ASLEAP Attack Detected

Alarm Description and Possible Causes

WLAN devices using static WEP key for encryption are vulnerable to the WEP key cracking attack (See *Weaknesses in the Key Scheduling Algorithm of RC4-I* by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information).

Cisco Systems introduced LEAP (Lightweight Extensible Authentication Protocol) to leverage the existing 802.1x framework to avoid such WEP key attacks. The Cisco LEAP solution provides mutual authentication, dynamic per session and per user keys, and configurable WEP session key time out. The LEAP solution was considered a stable security solution and is easy to configure.

There are hacking tools that compromise wireless LAN networks running LEAP by using off-line dictionary attacks to break LEAP passwords. After detecting WLAN networks that use LEAP, this tool de-authenticates users which forces them to reconnect and provide their username and password credentials. The hacker captures packets of legitimate users trying to reaccess 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 can 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 through 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 username and password credentials.

Some advantages of EAP-FAST include the following:

- 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 wIPS detects the deauthentication signature of the ASLEAP tool. When detected, the server alerts the wireless administrator. The user of the attacked station should reset the password. The best solution to counter the ASLEAP tool is to replace LEAP with EAP-FAST in the corporate WLAN environment.

NCS also provides automated security vulnerability scanning that proactively reports any access points configured to utilize weak encryption or authentication. For more information on automated security vulnerability scanning, see the NCS online Help.

Potential 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. When associated, the intruder performs attacks against the client station because traffic is diverted through the honey pot access point.

wIPS Solution

When a honey pot access point is identified and reported by the wIPS, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

Soft AP or Host AP Detected

Host AP tools: Cquire AP

Alarm Description and Possible Causes

A host-based access point (desktop or a laptop computer serving as a wireless access point) represents two potential threats to enterprise security. First, host based access points are not typically part of the enterprise wireless infrastructure and are likely to be rogue devices which do not conform to the corporate security policy. Second, host-based access points are used by wireless attackers as a convenient platform to implement various known intrusions such as man-in-the-middle, honey-pot access point, access point impersonation, and DoS (denial of service) attacks. Because software tools for turning a desktop or laptop into an access point can be easily downloaded from the Internet, host-based access points are more than just a theoretical threat.

Some laptops are shipped with the HostAP software preloaded and activated. When the laptops connect to the enterprise wireless network, they expose the wireless network to the hackers.

wIPS Solution

The wIPS's detected soft access point should be treated as a rogue access point as well as a potential intrusion attempt. When the soft access point is identified and reported by the wIPS, the WLAN administrator may use integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

Spoofed MAC Address Detected

Spoofing tools may include the following: SMAC, macchanger, and SirMACsAlot.

Alarm Description and Possible Causes

A wireless intruder can disrupt a wireless network using a wide range of available attack tools, many of which are available as free downloads from the Internet. Most of these tools rely on a spoofed MAC address which masquerades as an authorized wireless access point or as an authorized client. By using these tools, an attacker can launch various denial of service (DoS) attacks, bypass access control mechanisms, or falsely advertise services to wireless clients.

wIPS Solution

The wIPS detects a spoofed MAC address by following the IEEE authorized OUI (vendor ID) and 802.11 frame sequence number signature.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, see the *Cisco Wireless Control System Configuration Guide* or the NCS online Help.

Suspicious After-Hours Traffic Detected

Alarm Description and Possible Causes

One way to detect a wireless security penetration attempt is to match wireless usage against the time when there is not supposed to be any wireless traffic. The wIPS server monitors traffic patterns against the office-hours configured for this alarm to generate alerts when an abnormality is found. Specific suspicious wireless usage sought after by the wIPS server during after-office hours includes the following:

- Client station initiating authentication or association requests to the office WLAN that may indicate security breach attempts.
- Wireless data traffic that may indicate suspicious download or upload over the wireless network.

wIPS Solution

For global wIPS deployment, the configurable office-hour range is defined in local time. The access point or sensor can be configured with a time zone to facilitate management. For the office and manufacturing floor mixed WLAN, one can define one set of office hours for the office WLAN SSID and another set for the manufacturing floor WLAN SSID. If this alarm is triggered, the administrator should look for the devices responsible for the suspicious traffic and remove them from the wireless environment.

Unauthorized Association by Vendor List

Alarm Description and Possible Causes

In the enterprise WLAN environment, rogue stations cause security concerns and undermine network performance. They take up air space and compete for network bandwidth. Because an access point can only accommodate a limited number of stations, it rejects association requests from stations when its capacity is reached. An access point laden with rogue stations denies legitimate stations the access to the network. Common problems caused by rogue stations include connectivity problems and degraded performance.

wIPS Solution

The wIPS enables network administrators to include vendor information in a policy profile to allow the system to effectively detect stations in use on the WLAN that are not approved vendor products. An alarm is triggered.

When the alarm has been triggered, the unauthorized station must be identified and actions must be taken to resolve the issue. One way is to block it using the rogue containment.

Unauthorized Association Detected

Alarm Description and Possible Causes

In an enterprise network environment, rogue access points installed by employees do not usually follow the network'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. Because 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. Because 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 wIPS can automatically alert network administrators to any unauthorized access point-station association it has detected on the network through this alarm. When the alarm is triggered, the rogue or unauthorized device must be identified and actions must be taken to resolve the reported issue.

Wellenreiter Detected

Alarm Description and Possible Causes

The wIPS detects a wireless client station probing the WLAN for an anonymous association (such as association request for an access point with any SSID) using the Wellenreiter tool.

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) 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 <http://wellenreiter.sourceforge.net/index.html>

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the wIPS to see which of your access points is broadcasting an SSID in the beacons.

NCS also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, see the NCS online Help.

WiFiTap Tool Detected

Alarm Description & 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.



APPENDIX **B**

Rogue Management

This appendix describes security issues and solutions for rogue access points.

This appendix contains the following sections:

- [“Rogue Access Point Challenges” section on page B-1](#)
- [“Rogue Access Point Location, Tagging, and Containment” section on page B-1](#)
- [“Monitoring Alarms” section on page B-3](#)
- [“Configuring Controllers” section on page B-12](#)
- [“Configuring Controller Templates” section on page B-13](#)

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” section on page B-1](#).

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.
Set State to 'Known - External'—Tags the rogue access point as external, 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 under deployed 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, the 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, page B-3](#)
- [Monitoring Rogue Access Point Details, page B-5](#)
- [Detecting Access Points on a Network, page B-6](#)
- [Monitoring Events, page B-10](#)
- [Monitoring Rogue Clients, page B-11](#)

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.

Table N-1 describes the parameters found in the Rogue Access Point Alarms page.

Table N-1 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 MAC Address	Media Access Control address of the rogue access points. See Monitor Alarms > Rogue AP Details.
Vendor	Rogue access point vendor name, or Unknown.
Classification Type	Malicious, Friendly, or Unclassified.
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.
Owner	Indicates the `owner' of the rogue access point.
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 access point radio. (Blank if SSID is not broadcast.)
Map Location	Indicates the map location for this rogue access point.
Acknowledged	Displays whether or not the alarm is acknowledged by the user.

**Note**

The alarm remains in the Prime Infrastructure, and you can search for all Acknowledged alarms using the alarm search functionality.

Rogue AP Alarms page includes the following additional fields:

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- E-mail Notification—Takes you to the All Alarms > E-mail Notification page to view and configure e-mail notifications. See Monitor Alarms > E-mail Notification for more information.
- Severity Configuration—Change the severity level for newly-generated alarms. See Monitor Alarms > Severity Configuration for more information.
- Detecting APs—View the Cisco lightweight access points that are currently detecting the rogue access point.
- Map (High Resolution)—Click to display a high-resolution map of the rogue access point location.

- **Rogue Clients**—Click to view a list of rogue clients associated with this rogue access point. The Rogue Clients page displays the Client MAC address, when it was last heard, its current status, its controller, and the rogue access point.
- **Set State to `Unclassified - Alert`**—Choose this command to tag the rogue access point as the lowest threat, continue monitoring the rogue access point, and to turn off containment.
- **Set State to `Malicious - Alert`**—Choose this command to tag the rogue access point as Malicious.
- **Set State to `Friendly - Internal`**—Choose this command to tag the rogue access point as internal, add it to the Known Rogue APs list, and to turn off containment.
- **1 AP Containment**—Target the rogue access point for containment by one access point. (Lowest containment level.)
- **2 AP Containment**—Target the rogue access point for containment by two Cisco lightweight access points.
- **3 AP Containment**—Target the rogue access point for containment by three Cisco lightweight access points.
- **4 AP Containment**—Target the rogue access point for containment by four Cisco lightweight access points. (Highest containment level.)

**Caution**

Attempting to contain a rogue access point 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 Access Point 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 on a Network

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

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

-
- Step 1** To display the Rogue AP Alarms page, do one of the following:
- Perform a search for rogue APs. See the [“Using the Search Feature” section on page 2-34](#) for more information about the search feature.
 - From the Prime Infrastructure 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 AP on Network**.
- Step 4** Click **Go**.

Click a list item to display data about that item:

- AP Name
- Radio
- Map Location
- Detecting AP Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio.
- Channel Number—The channel on which the rogue access point is broadcasting.
- WEP—Enabled or disabled.

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

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 left sidebar menu, choose **New Search**, and choose **Rogue Adhoc** from the Alarm Category drop-down list. Click **Go** to display the matching alarms.
- Choose **Monitor > Security**. From the left sidebar menu, choose **Rogue Adhocs**.



Note

If there are multiple alarm page, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

[Table N-2](#) describes the fields found in the Rogue Ad hoc Alarms page.

Table N-2 *Rogue Ad hoc Alarms*

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.

Select a Command

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.
- Event History—Click to access the [Monitoring Events](#) page.
- 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. See the “[Detecting Access Points on a Network](#)” section on page B-6 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 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 802.11a**—Whether or not the rogue access point is broadcasting on the 802.11a band.
- **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.

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 Switch Port Tracing Criteria on the 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, page B-13](#)
- [Configuring Rogue AP Rules, page B-13](#)

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 Prime Infrastructure 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. See the “[Configuring Rogue AP Rules](#)” section on [page B-15](#) for more information.
-

Configuring Controller Templates

This section contains the following topics:

- [Configuring Rogue Policies](#)
- [Configuring Rogue AP Rules](#)
- [Configuring Rogue AP Rule Groups](#)

Configuring Rogue Policies

This page enables you to configure the rogue policy template (for access points and clients) applied to the controller.

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 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 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 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—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 create a new Rogue AP Rule Groups template, 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 the [“Configuring Rogue AP Rules”](#) section on page B-15 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.



Radio Resource Management

The operating system security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access point, and automatically discover and locate rogue access points.

RRM is built into the Cisco Unified Wireless Network monitors and dynamically corrects performance issues found in the RF environment.

This appendix contains the followings sections:

- [“RRM Dashboard” section on page C-1](#)
- [“Configuring Controllers” section on page C-4](#)
- [“Configuring Controller Templates” section on page C-6](#)

RRM Dashboard

RRM automatically detects and configures new controllers and lightweight access points as they are added to the network. It then automatically adjusts associated and nearby lightweight access points to optimize coverage and capacity.

Lightweight access points can simultaneously scan all valid 802.11a/b/g channels for the country of operation as well as for channels available in other locations. The access points go “off-channel” for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

**Note**

In the presence of voice traffic (in the last 100 ms), the access points defer off-channel measurements and do not change channels.

Each access point spends only 0.2 percent of its time off-channel. This activity is distributed across all access points so that adjacent access points are not scanning at the same time, which can adversely affect wireless LAN performance. In this way, administrators gain the perspective of every access point, thereby increasing network visibility.

The Prime Infrastructure provides a snapshot of RRM statistics to help identify trouble spots and possible reasons for channel or power level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on grouping the events together (access point performance, configuration mismatch between controllers in the same RF group, coverage holes that were detected by access points based on threshold, coverage holes that were detected by controllers, ratios of access points operating at maximum power, and so on).



Note The RRM dashboard information is only available for CAPWAP access points.

This section contains the following topics:

- [Channel Change Notifications, page C-2](#)
- [Transmission Power Change Notifications, page C-3](#)
- [RF Grouping Notifications, page C-3](#)
- [Viewing the RRM Dashboard, page C-3](#)

Channel Change Notifications

Two adjacent access points on the same channel can cause either a signal contention or signal collision. In the case of a collision, data is simply not received by the access point. This functionality can become a problem, for example, when someone reading e-mail in a cafe affects the performance of the access point in a neighboring business. Even though these are completely separate networks, someone sending traffic to the cafe on channel 1 can disrupt communication in an enterprise using the same channel. Controllers address this problem by dynamically allocating access point channel assignments to avoid conflict and to increase capacity and performance. Channels are “reused” to avoid wasting scarce RF resources. In other words, channel 1 is allocated to a different access point far from the cafe, which is more effective than not using channel 1 altogether.

The Dynamic Channel Assignment (DCA) capabilities of controllers are also useful in minimizing adjacent channel interference between access points. For example, two overlapping channels in the 802.11b/g band, such as 1 and 2, cannot both simultaneously use 11/54 Mb/s. By effectively reassigning channels, the controller keeps adjacent channels separated, thereby avoiding this problem.

Notifications are sent to the Prime Infrastructure RRM dashboard when a channel change occurs. Channel changes depend on the DCA configuration where the mode can be set to auto or on demand. When the mode is *auto*, channel assignment is periodically updated for all CAPWAP access points which permit this operation. When the mode is set to *on demand*, channel assignments are updated based upon request. If the DCA is static, no dynamic channel assignments occur, and values are set to their global default.

DCA supports 802.11n 40-MHz channels in the 5-GHz band. 40-MHz channelization allows radios to achieve higher instantaneous data rates (potentially 2.25 times higher than 20-MHz channels.) You can choose between DCA working at 20 or 40 MHz.



Note Radios using 40-MHz channelization in the 2.4-GHz band are not supported by DCA.

When a channel change trap is received and a channel change had occurred earlier, the event is marked as Channel Revised; otherwise, the event is marked as Channel Changed. Each event for a channel change can be caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur. For example, suppose a channel change is caused by signal, interference, or noise. When the reason code is received in the notification, the reason code is refactored across the reasons. If three reasons caused the event to occur, the reason code is refactored to 1/3 or 0.33 per reason. If ten channel change events are received with the same reason code, all of the three reasons are equally factored to determine the cause of the channel change.

Transmission Power Change Notifications

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the access point transmit power according to how the access points are seen by their third strongest neighbor.

The transmit power control algorithm only reduces the power of an access point. However, the coverage hole algorithm can increase access point power, thereby filling a coverage hole. For example, if a failed access point is detected, the coverage hole algorithm can automatically increase power on surrounding access points to fill the gap created by the loss in coverage.

Notifications are sent to the Prime Infrastructure RRM dashboard when transmission power changes occur. Each event for transmit power changes is caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur.

RF Grouping Notifications

When RRM is run on the controller, dynamic grouping is done, and a new group leader is chosen. Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs, and each switch optimizes only its own CAPWAP access point parameters. When the grouping is on, switches form groups and elect leaders to perform better dynamic parameter optimization. With grouping on, configured intervals (in seconds) represent the period with which the grouping algorithm is run. (Grouping algorithms also run when the group contents change and automatic grouping is enabled.)

Viewing the RRM Dashboard

The RRM dashboard is accessed by choosing **Monitor > RRM**.

The RRM dashboard includes the following information:

- The RRM Statistics shows network-wide statistics.
- The Channel Change Reason shows why channels changed for all 802.11a/b/g/n radios.
- The Channel Change shows all events complete with causes.
- The Configuration Mismatch shows comparisons between the leaders and members.
- The Coverage Hole rates how severe the coverage holes are and gives their location.
- The Percent Time at Maximum Power shows what percent of time the access points were at maximum power and gives the location of those access points.

The following statistics are displayed:

- **Total Channel Changes**—The sum total of channel changes across 802.11a/b/g/n radios, irrespective of whether the channel was updated or revised. The count is split over a 24-hour and 7-day period. If you click the percentages link or the link under the 24-hour column, a page with details for that access point only appears.
- **Total Configuration Mismatches**—The total number of configuration mismatches detected over a 24-hour.
- **Total Coverage Hole Events**—The total number of coverage hole events over a 24-hour and 7-day period.

- **Number of RF Groups**—The total number of RF groups currently managed by the Prime Infrastructure.
- **Configuration Mismatch**—The configuration mismatch over a 24-hour period by RF group with details on the group leader.
- **Percent of APs at MAX Power**—The percentage of access points with 802.11a/n radios as a total percentage across all access points which are at maximum power. The maximum power levels are preset and are derived with reference to the present maximum power of the access point.



Note Maximum power is shown in three areas of the RRM dashboard. This maximum power portion shows the current value and is poll driven.

- **Channel Change Causes**—A graphical bar chart for 802.11a/n radios. The chart is factored based on the reason for channel change. The chart is divided into two parts, each depicting the percentage of weighted reasons causing the event to occur over a 24-hour and 7-day period. Each event for channel change can be caused by multiple reasons, and the weight is equally divided across these reasons. The net reason code is factored and equated to one irrespective of the number of reasons for the event to occur.
- **Channel Change APs**—Each event for channel change includes the MAC address of the CAPWAP access point. For each reason code, you are given the most channel changes that occurred for the 802.11a/n access point based on the weighted reason for channel events. This count is split over a 24-hour and 7-day period.
- **Coverage Hole Events APs**—The top five access points filtered by IF Type 11 a/n which triggered a coverage hole event are displayed.
- **Aggregated Percent Max Power APs**—A graphical progressive chart of the total percentage of 802.11a/n CAPWAP access points which are operating at maximum power to accommodate coverage holes and events. The count is split over a 24-hour and 7-day period.



Note This maximum power portion shows the values from the last 24 hours and is poll driven. The power is polled every 15 minutes or as configured for radio performance.

- **Percent Time at Maximum Power**—A list of the top five 802.11a/n CAPWAP access points which have been operating at maximum power.



Note This maximum power portion shows the value from the last 24 hours and is only event driven.

Configuring Controllers

This section contains the following topics:

- [Configuring an RRM Threshold Controller \(for 802.11a/n or 802.11b/g/n\), page C-5](#)
- [Configuring 40-MHz Channel Bonding, page C-5](#)

Configuring an RRM Threshold Controller (for 802.11a/n or 802.11b/g/n)

To configure an 802.11a/n or 802.11b/g/n RRM threshold controller, follow these steps:

-
- Step 1** Choose **Configure > Controller**.
 - Step 2** Click the IP address of the appropriate controller to open the Controller Properties page.
 - Step 3** From the left sidebar menu, choose **802.11a/n > RRM Thresholds** or **802.11b/g/n > RRM Thresholds**.
 - Step 4** Make any necessary changes to Coverage Thresholds, Load Thresholds, Other Thresholds, and Noise/Interference/Rogue Monitoring Channels.

**Note**

When the Coverage Thresholds Min SNR Level (dB) parameter is adjusted, the value of the Signal Strength (dB) automatically reflects this change. The Signal Strength (dB) parameter provides information regarding what the target range of coverage thresholds is when adjusting the SNR value.

-
- Step 5** Click **Save**.

Configuring 40-MHz Channel Bonding

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.

**Note**

Choosing a larger bandwidth reduces the non-overlapping channels which can potentially reduce the overall network throughput for certain deployments.

To configure 802.11 a/n RRM DCA channels for an individual controller, follow these steps:

-
- Step 1** Choose **Configure > Controllers**.
 - Step 2** Click the IP address of the appropriate controller.
 - Step 3** From the left sidebar menu, choose **802.11a/n > RRM DCA**. The 802.11a/n RRM DCA page appears.

**Note**

You can also configure the channel width on the access point page by choosing **Configure > Access Points** and clicking the **802.11a/n** link in the Radio column. The Current RF Channel Assignment is provided, and you can choose a Global assignment method or choose Custom to specify a channel.

-
- Step 4** From the Channel Width drop-down list, choose **20 MHz** or **40 MHz**.

**Note**

Be cautious about deploying a mix of 20-MHz and 40-MHz devices. The 40-MHz devices have slightly different channel access rules, which may negatively impact the 20-MHz devices.



Note To view the channel width for the radio of an access point, choose **Monitor > Access Points > name > Interfaces** tab. You can also view the channel width and antenna selections by choosing **Configure > Access Points** and clicking the desired radio in the Radio column.

- Step 5** Select the check box(es) for the applicable DCA channel(s). The selected channels are listed in the Selected DCA channels text box.
- Step 6** Click **Save**.

Configuring Controller Templates

This section contains the following topics:

- [Configuring an RRM Threshold Template for 802.11a/n or 802.11b/g/n, page C-6](#)
- [Configuring an RRM Interval Template \(for 802.11a/n or 802.11b/g/n\), page C-7](#)

Configuring an RRM Threshold Template for 802.11a/n or 802.11b/g/n

To add a new 802.11a/n or 802.11b/g/n RRM threshold template or make modifications to an existing template, follow these steps:

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **802.11a/n > RRM Thresholds** or **802.11b/g/n > RRM Thresholds**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To make modifications to an existing template, click a template name in the Template Name column. The 802.11a/n or 802.11b/g/n RRM Thresholds Template page appears and the number of controllers the template is applied to automatically populates.
- Step 4** Enter the minimum number of failed clients that are currently associated with the controller.
- Step 5** Enter the desired coverage level. When the measured coverage drops by the percentage configured in the coverage exception level, a coverage hole is generated.
- Step 6** The Signal Strength (dBm) parameter shows the target range of coverage thresholds.
- Step 7** Enter the maximum number of clients currently associated with the controller.
- Step 8** In the RF Utilization text box, enter the percentage of threshold for either 802.11a/n or 802.11b/g/n.
- Step 9** Enter an interference threshold.
- Step 10** Enter a noise threshold between -127 and 0 dBm. When outside of this threshold, the controller sends an alarm to the Prime Infrastructure.
- Step 11** Enter the coverage exception level percentage. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole is generated.
- Step 12** From the Channel List drop-down list in the Noise/Interference/Rogue Monitoring Channels section, choose **all channels**, **country channels**, or **DCA channels** based on the level of monitoring you want. Dynamic Channel Assignment (DCA) automatically selects a reasonably good channel allocation among a set of managed devices connected to the controller.

Step 13 Click **Save**.

Configuring an RRM Interval Template (for 802.11a/n or 802.11b/g/n)

To add an 802.11a/n or 802.11b/g/n RRM interval template or make modifications to an existing template, follow these steps:

-
- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **802.11a/n > RRM Intervals** or **802.11b/g/n > RRM Intervals**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To make modifications to an existing template, click a template name in the Template Name column. The 802.11a/n or 802.11b/g/n RRM Threshold Template appears and the number of controllers the template is applied to automatically populates.
- Step 4** Enter at which interval you want strength measurements taken for each access point. The default is 300 seconds.
- Step 5** Enter at which interval you want noise and interference measurements taken for each access point. The default is 300 seconds.
- Step 6** Enter at which interval you want load measurements taken for each access point. The default is 300 seconds.
- Step 7** Enter at which interval you want coverage measurements taken for each access point. The default is 300 seconds.
- Step 8** Click **Save**.
-

A

adding 1, 3

alarm notifications

 emailing 5

assigning location presence 35

audit report

 for alarms 4

automatic backup 4

automatic synchronization 6

B

backup historical data 3

buildings

 adding to NCS database 36

C

civic address 36

clear 5

configuring 7, 6

Current building

 delete 38

 edit map 38

D

deleting 2, 3

download 8

E

edit location presence information 35

editing 1

event history 4

F

failover 2

G

general properties 1

H

high availability 1

I

identity client 32

L

licensing for MSAP 1

location presence

 assigning 35

M

monitor alarms

 Rogue APs 7

MSAP 1

- MSAP provisioning 2
- MSAP reports 6
- N
- network designs 1
- NTP Server
 - Configuring 6
- O
- out-of-sync 7
- P
- pairing matrix 2
- permission 2
- properties 4
- R
- recovering lost 1
- restore historical data 3
- rogue policies
 - templates 14
- S
- scheduled tasks 6
- service advertisement synchronization 6
- service advertisements 4
- software download 4
- synchronization 7
- synchronization history 8
- T
- templates
 - controller
 - rogue policies 14
- V
- viewing 2, 6
- viewing HA parameters 6
- viewing HA status 7
- viewing MSAP statistics 5