# Cisco Adaptive Wireless Intrusion Prevention System Configuration Guide

Release 7.0.x

April 2011

**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-23941-01

*Cisco Adaptive Wireless Intrusion Prevention System Configuration Guide*

# CONTENTS

Preface xi

Objectives xi

Audience xi

Conventions xi

Related Documentation xiii

Obtaining Documentation and Submitting a Service Request xiii

CHAPTER 1 Overview 1-1

Overview of wIPS 1-1

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 1-4

wIPS Overlay in Autonomous or Other Wireless Network 1-6

Differences Between Controller IDS and Adaptive wIPS 1-6

Reduction in False Positives 1-7

Alarm Aggregation 1-7

DoS Attacks 1-8

Security Penetration Attacks 1-8

wIPS Alarm Flow 1-9

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 Overview 1-12

Adding and Deleting Mobility Services Engine 1-12

Editing Mobility Services Engine Properties 1-12

Managing Users and Groups 1-12

Mobility Services Engine Synchronization 1-13

Configuring wIPS and Profile Management 1-13

Monitoring Capability 1-13

Maintenance Operations 1-13

MSE System and Appliance Hardening 1-13

System Compatibility 1-13

CHAPTER 2 Adding and Deleting Systems 2-1

Adding a Mobility Services Engine to WCS 2-1

Deleting a Mobility Services Engine from the Cisco WCS 2-2

MSE License Overview 2-3

MSE License Structure Matrix 2-3

Sample MSE License File 2-3

Revoking and Reusing an MSE License 2-4

Revoking an MSE License Using MSE CLI 2-4

Registering Client and wIPS Product Authorization Keys 2-4

Installing wIPS License Files 2-9

CHAPTER 3 Synchronizing Mobility Services Engines 3-1

Synchronizing WCS and Mobility Services Engines 3-1

Synchronizing Controllers with a Mobility Services Engine 3-4

Working with Third-Party Elements 3-5

Configuring Automatic Database Synchronization and Out-of-Sync Alerts 3-5

Smart Controller Assignment and Selection Scenarios 3-6

Out-of-Sync Alarms 3-7

Viewing Synchronization Information 3-7

Viewing Mobility Services Engine Synchronization Status 3-7

Viewing Synchronization History 3-8

CHAPTER 4 Configuring and Viewing System Properties 4-1

Editing General Properties and Viewing Performance 4-1

Editing General Properties 4-1

Viewing Performance Information 4-4

Modifying NMSP Parameters 4-5

Viewing Active Sessions on a System 4-7

Adding and Deleting Trap Destinations 4-7

Adding Trap Destinations 4-7

Deleting Trap Destinations 4-8

Viewing and Configuring Advanced Parameters 4-9

Viewing Advanced Parameters Settings 4-9

Initiating Advanced Parameters 4-10

Configuring Advanced Parameters 4-10

Initiating Advanced Commands 4-11

Rebooting or Shutting Down a System 4-11

Clearing the System Database 4-12

CHAPTER 5 Managing Users and Groups 5-1

Managing Groups 5-1

Adding User Groups 5-1

Deleting User Groups 5-2

Changing User Group Permissions 5-2

Managing Users 5-2

Adding Users 5-3

Deleting Users 5-4

Changing User Properties 5-4

CHAPTER 6 Configuring wIPS and Profiles 6-1

Overview of wIPS Configuration and Profile Management 6-1

Configuring Access Points for wIPS Monitor Mode 6-2

Configuring wIPS Profiles 6-4

CHAPTER 7 Monitoring the System and Services 7-1

Working with Alarms 7-2

Viewing Alarms 7-2

Viewing MSE Alarm Details 7-3

Assigning and Unassigning Alarms 7-5

Deleting and Clearing Alarms 7-6

Emailing Alarm Notifications 7-6

Working with Events 7-8

Working with Logs 7-8

Configuring Logging Options 7-9

MAC Address Based Logging 7-9

Downloading Log Files 7-10

Generating Reports 7-10

Creating a Device Utilization Report 7-10

Viewing Saved Utilization Reports 7-13

Viewing Scheduled Utilization Runs 7-13

Security Reports and Alarms for wIPS 7-14

Creating a New wIPS Security or Alarms Report 7-15

Viewing Saved wIPS Report 7-17

Viewing Scheduled wIPS Report Runs 7-17

CHAPTER 8 Performing Maintenance Operations 8-1

Recovering a Lost Password 8-1

Recovering a Lost Root Password **8-2**

Backing Up and Restoring Mobility Services Engine Data **8-2**

Backing Up Mobility Services Engine Historical Data **8-2**

Restoring Mobility Services Engine Historical Data **8-3**

Enabling Automatic Data Backup **8-4**

Downloading Software to Mobility Services Engines **8-4**

Manually Downloading Software **8-5**

Configuring the NTP Server **8-6**

Resetting the System **8-6**

Clearing the Configuration File **8-6**

APPENDIX A **wIPS Policy Alarm Encyclopedia** **A-1**

Security IDS/IPS Overview **A-1**

Intrusion Detection—Denial of Service Attack **A-2**

Denial of Service Attack Against Access Points **A-3**

Denial of Service Attack: Association Flood **A-3**

Denial of Service Attack: Association Table Overflow **A-4**

Denial of Service Attack: Authentication Flood **A-5**

Denial of Service Attack: EAPOL-Start Attack **A-6**

Denial of Service Attack: PS Poll Flood Attack **A-6**

Denial of Service Attack: Unauthenticated Association **A-7**

Denial of Service Attack Against Infrastructure **A-8**

Denial of Service Attack: CTS Flood **A-8**

Denial of Service Attack: Queensland University of Technology Exploit **A-9**

Denial of Service attack: RF Jamming Attack **A-10**

Denial of Service: RTS Flood **A-11**

Denial of Service Attack: Virtual Carrier Attack **A-11**

Denial of Service Attacks Against Client Station **A-12**

Denial of Service Attack: Authentication Failure Attack **A-12**

Denial of Service Attack: Deauthentication Broadcast **A-13**

Denial of Service Attack: Deauthentication Flood **A-14**

Denial of Service Attack: Disassociation Broadcast **A-15**

Denial of Service Attack: Disassociation Flood **A-16**

Denial of Service Attack: EAPOL Logoff Attack **A-18**

Denial of Service Attack: FATA Jack Tool Detected **A-18**

Denial of Service Attack: Premature EAP Failure Attack **A-20**

Denial of Service Attack: Premature EAP Success Attack **A-21**

Intrusion Detection—Security Penetration **A-21**

Airsnarf Attack Detected **A-23**

Potential Chopchop Attack in Progress A-24
Day-0 Attack by WLAN Performance Anomaly A-24
Day-0 Attack by WLAN Security Anomaly A-26
Day-0 Attack by Device Performance Anomaly A-27
Day-0 Attack by Device Security Anomaly A-29
Device Probing for Access Points A-30
Dictionary Attack on EAP Methods A-32
EAP Attack Against 802.1x Authentication A-32
Fake Access Points Detected A-33
Fake DHCP Server Detected (Potential Wireless Phishing) A-33
Fast WEP Crack (ARP Replay) Detected A-34
Potential Fragmentation Attack in Progress A-35
Hot-Spotter Tool Detected (Potential Wireless Phishing) A-35
Malformed 802.11 Packets Detected A-36
Man-in-the-Middle Attack Detected A-37
Monitored Device Detected A-38
NetStumbler Detected A-38
NetStumbler Victim Detected A-39
Publicly Secure Packet Forwarding (PSPF) Violation A-39
Potential ASLEAP Attack Detected A-40
Potential Honeypot AP Detected A-42
Soft AP or Host AP Detected A-42
Spoofed MAC Address Detected A-42
Suspicious After-Hours Traffic Detected A-43
Unauthorized Association by Vendor List A-43
Unauthorized Association Detected A-44
Wellenreiter Detected A-44

APPENDIX B **Rogue Management** B-1
Rogue Access Point Challenges B-1
Rogue Access Point Location, Tagging, and Containment B-1
Detecting and Locating Rogue Access Points B-2
Monitoring Alarms B-3
Monitoring Rogue Access Point Alarms B-3
Monitoring Rogue Access Point Details B-5
Detecting Access Points B-6
Monitoring Rogue Adhoc Alarms B-7
Monitoring Rogue Adhoc Details B-8
Monitoring Events B-10

Monitoring Rogue Clients B-11

Configuring Controllers B-11

Configuring Rogue Policies B-11

Configuring Rogue AP Rules B-12

Configuring Controller Templates B-12

Configuring Rogue Policies B-12

Configuring Rogue AP Rules B-13

Configuring Rogue AP Rule Groups B-15

APPENDIX C Radio Resource Management C-1

RRM Dashboard C-1

Channel Change Notifications C-2

Transmission Power Change Notifications C-3

RF Grouping Notifications C-3

Viewing the RRM Dashboard C-3

Configuring Controllers C-4

Configuring an RRM Threshold Controller (for 802.11a/n or 802.11b/g/n) C-5

Configuring 40-MHz Channel Bonding C-5

Configuring Controller Templates C-6

Configuring an RRM Threshold Template for 802.11a/n or 802.11b/g/n C-6

Configuring an RRM Interval Template (for 802.11a/n or 802.11b/g/n) C-7

APPENDIX D MSE System and Appliance Hardening Guidelines D-1

Setup Wizard Update D-1

Configure future restart day and time D-1

Configure Remote Syslog Server to publish MSE logs D-2

Configure Host access control settings D-2

Certificate Management D-2

Create a CSR D-3

Import CA Certificate D-4

Import Server Certificate D-4

Enable or Disable Client Certificate Validation D-5

OCSP Settings D-5

Import a CRL D-6

Clear Certificate Configuration D-6

Show Certificate Configuration D-7

WCS GUI Updates for SNMPv3 D-10

Updated Open Port List D-10

Syslog Support D-10

MSE and RHEL 5 D-11

INDEX

# Preface

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

- Objectives, page xi
- Audience, page xi
- Conventions, page xi
- Related Documentation, page xiii
- Obtaining Documentation and Submitting a Service Request, page xiii

## Objectives

This guide describes how to use the Cisco Wireless Control System (WCS) to configure and manage the Cisco 3310 mobility services engine and the Cisco Adaptive Wireless Intrusion Prevention System (wIPS), which 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:

- Command 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 screen 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.

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

**Warning** **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix “Translated Safety Warnings.”)**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico’s en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel “Translated Safety Warnings” (Vertalingen van veiligheidsvoorschriften) raadplegen.)**

Varoitus **Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)**

Attention **Ce symbole d’avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d’accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l’annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel “Translated Safety Warnings” (Übersetzung der Warnhinweise).)**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell’appendice, “Translated Safety Warnings” (Traduzione delle avvertenze di sicurezza).**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)**

# Related Documentation

See the *Cisco 3310 Mobility Services Engine Getting Started Guide*, which describes how to install and set up mobility services engines.

This document is available on the Cisco.com website 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*, which also lists all new and revised Cisco technical documentation, at:

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

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

CHAPTER 1

# Overview

This chapter describes the role of the Cisco 3300 series 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:

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

## Overview of wIPS

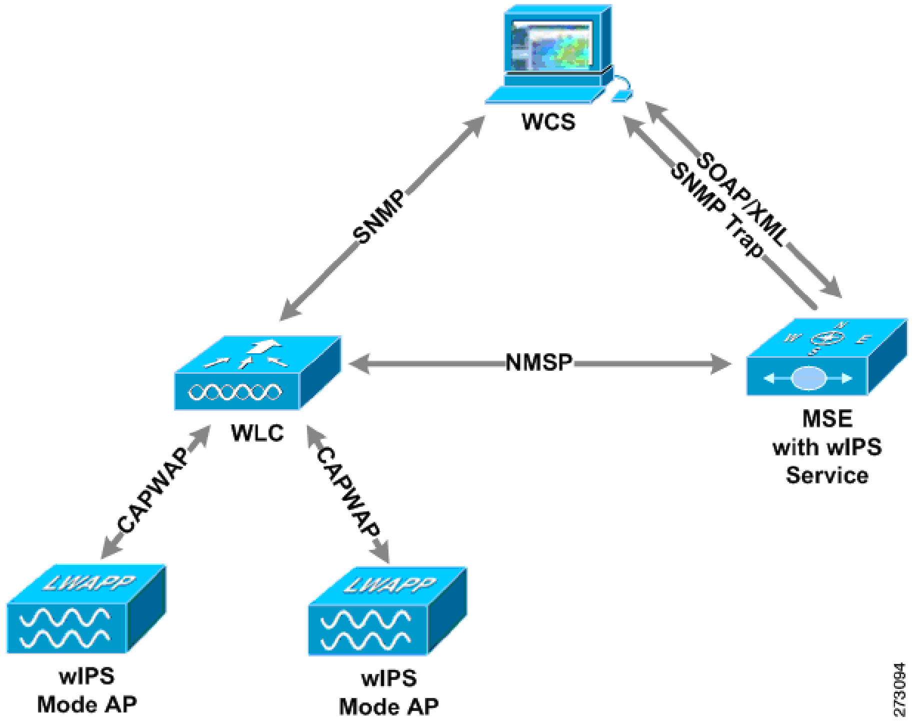
The wIPS performs rogue access point, rogue client, and ad-hoc connection detection and mitigation, over-the-air wireless hacking and threat detection, security vulnerability monitoring, performance monitoring and self-optimization, network hardening for proactive prevention of threats, and complete 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 monitor mode access points. Alarm information and forensic files are stored on the mobility services engine for archival purposes.
- A wIPS monitor mode access point—Provides constant channel scanning with attack detection and forensics (packet capture) capabilities.
- Local mode access point—Provides wireless service to clients in addition to time-sliced rogue scanning.
- Wireless LAN Controller—Forwards attack information received from wIPS monitor mode access points to the mobility services engine and distributes configuration parameters to access points.

- Wireless Control System (WCS)—Provides a centralized management platform for the administrator to configure the wIPS Service on the mobility services engine, push wIPS configurations to the controller, and configure access points in wIPS monitor mode. WCS is also used to view wIPS alarms, forensics, reporting, and to access the attack encyclopedia. (See Figure 1-1).

***Figure 1-1 Wireless Intrusion Prevention System***



**Note** The HREAP mode access points also support wIPS.

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 WCS. This protocol is used to distribute configuration parameters to the wIPS service running on the mobility services engine.
  - MSE TCP Port: 443
- Simple Network Management Protocol (SNMP)—This protocol is used to forward wIPS alarm information from the mobility services engine to the WCS. It is also employed to communicate rogue access point information from the controller to WCS.

# wIPS in a Cisco Unified Wireless Network

You can integrate wIPS within the CUWN infrastructure or overlay wIPS on the CUWN or Cisco autonomous wireless network (or third-party wireless network).

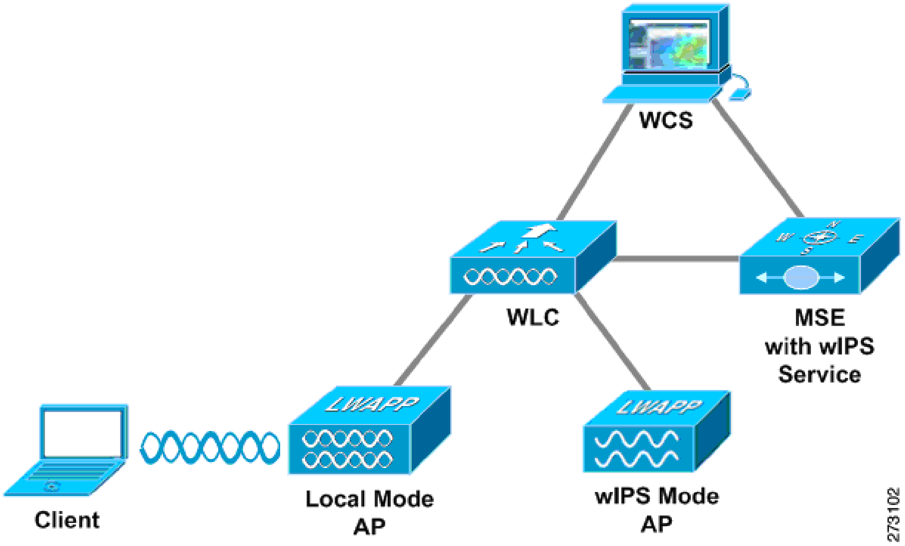
This section contains the following topics:

- wIPS Integrated Within a Cisco Unified Wireless Network, page 1-3
- wIPS Overlay Deployment in a Cisco Unified Wireless Network, page 1-4
- wIPS Overlay in Autonomous or Other Wireless Network, page 1-6

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

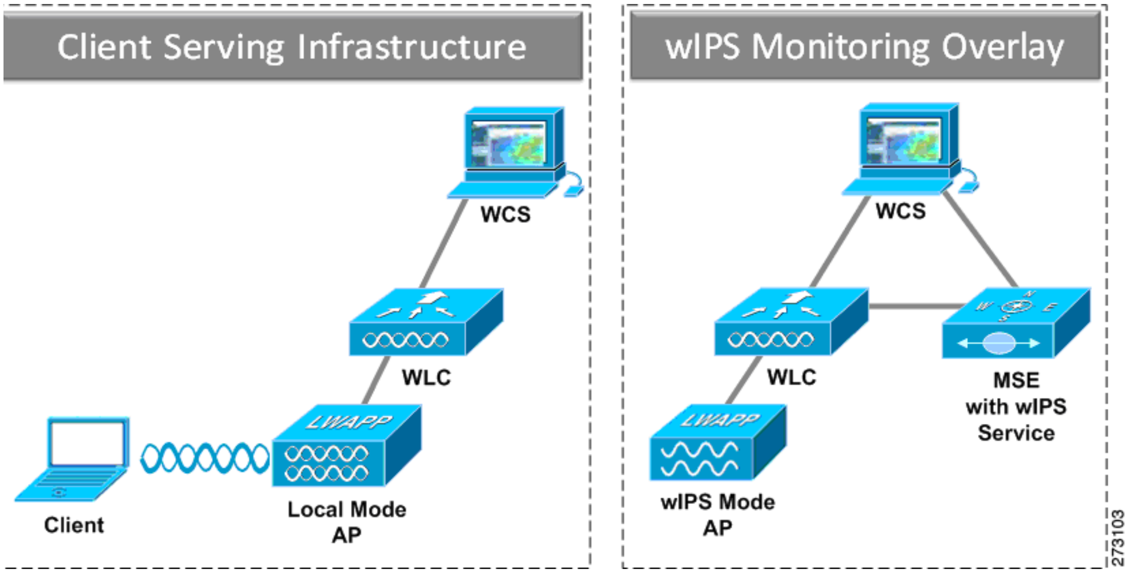
*Figure 1-2 wIPS Integrated Within CUWN*



## wIPS Overlay Deployment in a Cisco Unified Wireless Network

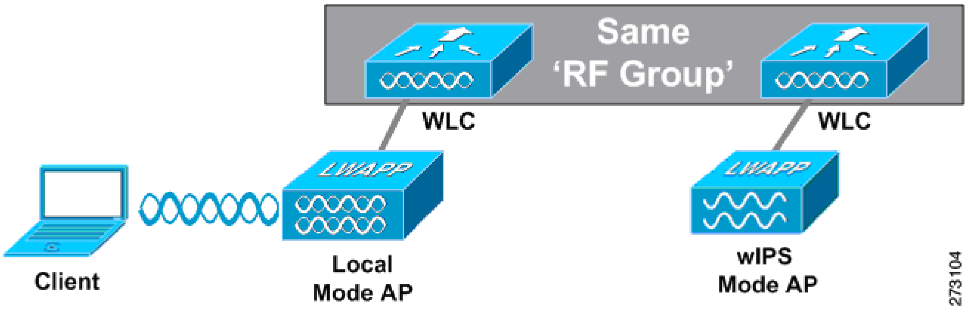
In a wIPS Overlay deployment, the wIPS monitoring infrastructure is completely separate from the client serving infrastructure. Each distinct system has its own set of controllers, access points and WCS. The reason for selecting this deployment model often stems from business mandates that require distinct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

*Figure 1-3 wIPS Overlay Monitoring Network Deployment in CUWN*



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 Deployment*



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

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

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

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

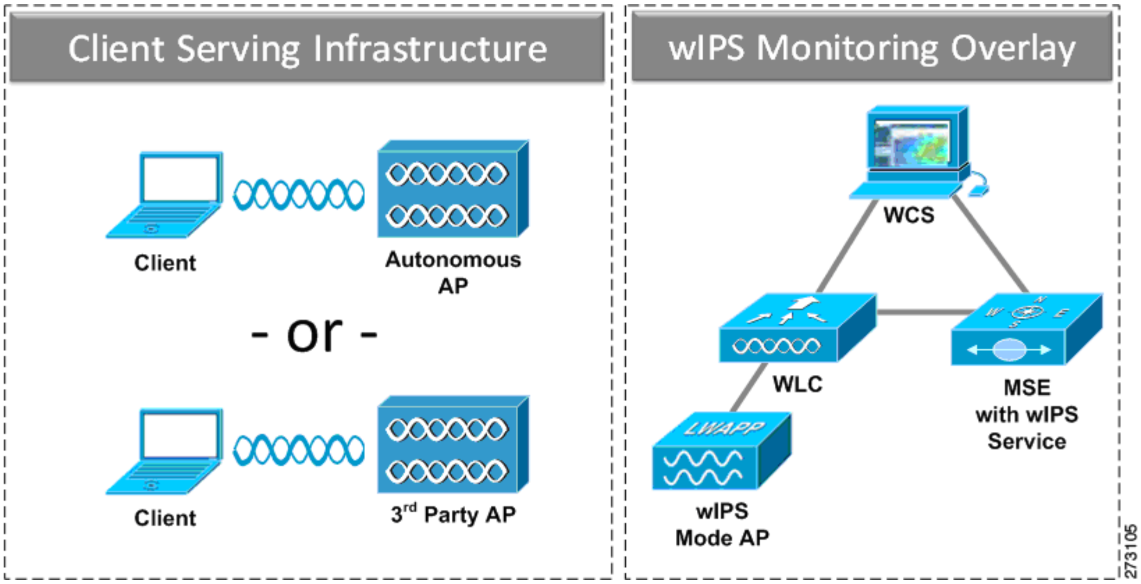
| | Client Serving Infrastructure WCS | wIPS Monitoring Overlay WCS |
|---|---|---|
| wIPS alarms | No | Yes |
| MFP alarms | Yes | No |
| Rogue alarms | Yes | Yes |
| Rogue location | High accuracy | Low accuracy |
| Rogue containment | Yes | Yes, but scalable |

One challenge of the overlay solution is the possibility of lightweight access points on either the client serving infrastructure or wIPS monitoring overlay associating to the wrong controller. Association with the wrong controller can be addressed by specifying the primary, secondary and tertiary controller names for each access point (both local and wIPS monitor mode). In addition, 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 Autonomous or Other Wireless Network

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

***Figure 1-5 wIPS Overlay in Autonomous***



# Differences Between Controller IDS and Adaptive wIPS

This section contains the following topics:

- 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

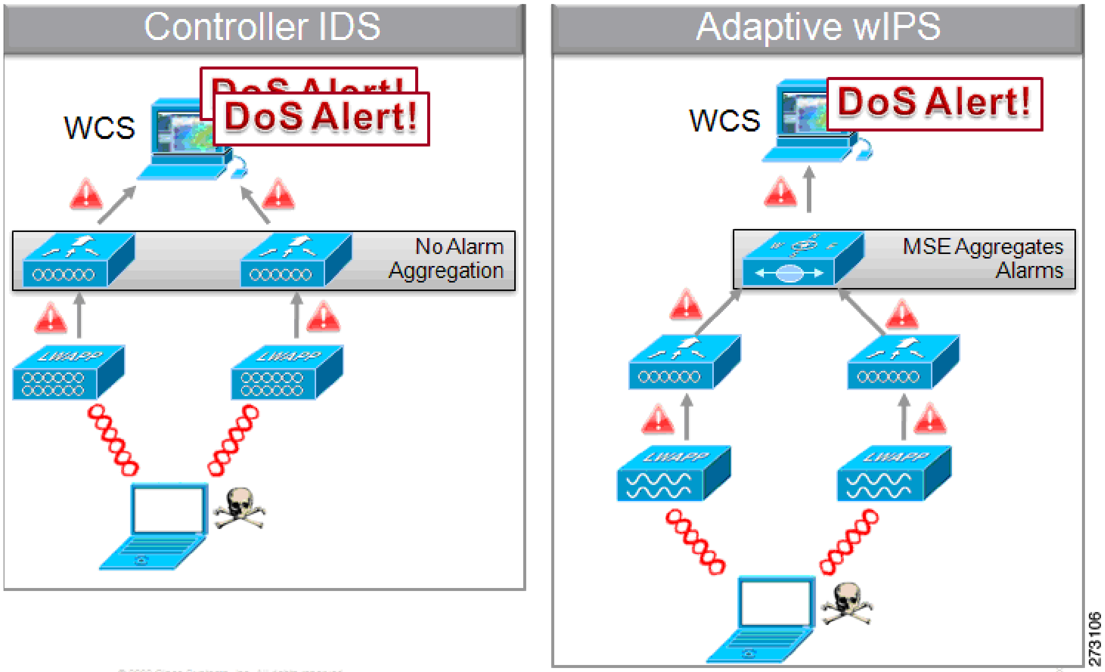
## Reduction in False Positives

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 a result of the wIPS system being able to dynamically identify the state and validity of access points and clients present in the wireless infrastructure. Only when attacks are launched against the infrastructure are alarms raised.

## Alarm Aggregation

One major differentiation between the existing controller-based IDS system of Cisco 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 will only be forwarded to the WCS once because alarm aggregation takes place on the mobility services engine. The existing controller-based IDS system does not aggregate alarms (Figure 1-6).

*Figure 1-6 Alarm Aggregation Using Controller-based IDS of Cisco versus Adaptive wIPS*



Another major differentiation between the controller-based IDS and wIPS is the number of attacks that each system can detect. As described in the sub-sections and showcased in the tables 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.

## 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, they do not result in a data breach and their negative consequences are often over once the attack has stopped. Table 1-2 compares the DoS attacks detected by the controller-based IDS and wIPS service.

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

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

## Security Penetration Attacks

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

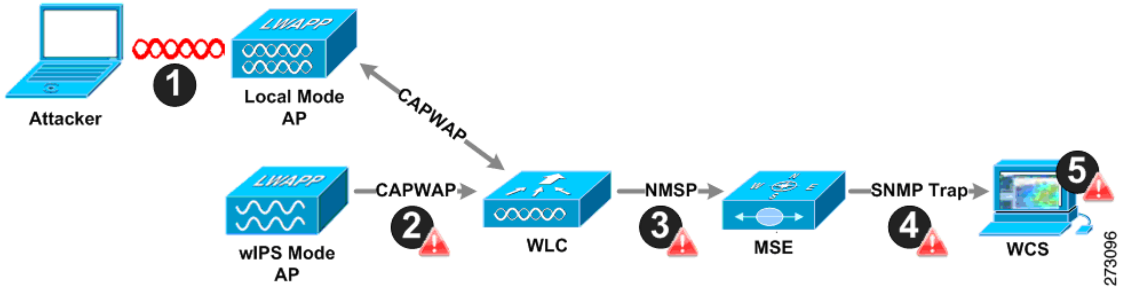
*Table 1-3 Security Penetration Attack Detection by Controller IDS and wIPS*

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

*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 WCS. The SNMP trap contains the attack information. If multiple alarm updates are received referencing the same attack (for example, if multiple access points hear the same attack) only one SNMP trap is sent to WCS.
5. The SNMP trap containing the alarm information is received and displayed by WCS.

# Forensics

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

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

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

## Rogue Detection

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

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

## Anomaly Detection

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

## Default Configuration Profiles

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

## Integration into Release 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 under their own category.

# Configuration Overview

This guide addresses the configuration of wIPS and mobility services engine. This section lists and describes the following topics:

- Adding and Deleting Mobility Services Engine, page 1-12
- Editing Mobility Services Engine Properties, page 1-12
- Managing Users and Groups, page 1-12
- Mobility Services Engine Synchronization, page 1-13
- Configuring wIPS and Profile Management, page 1-13
- Monitoring Capability, page 1-13
- Maintenance Operations, page 1-13
- MSE System and Appliance Hardening, page 1-13
- System Compatibility, page 1-13

## Adding and Deleting Mobility Services Engine

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

## Editing Mobility Services Engine Properties

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

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

## Managing Users and Groups

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

## Mobility Services Engine Synchronization

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

## Configuring wIPS and Profile Management

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

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

## Monitoring Capability

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

## Maintenance Operations

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

## MSE System and Appliance Hardening

The System and Appliance Hardening requires some services and processes to be exposed to function properly. Hardening of MSE would involve disabling unnecessary services, upgrading to latest server versions, and applying appropriate restrictive permissions to files, services, and end points. See Appendix D, "MSE System and Appliance Hardening Guidelines".

## System Compatibility

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

CHAPTER 2

# Adding and Deleting Systems

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

This chapter contains the following sections:

- Adding a Mobility Services Engine to WCS, page 2-1
- Deleting a Mobility Services Engine from the Cisco WCS, page 2-2
- MSE License Overview, page 2-3
- Registering Client and wIPS Product Authorization Keys, page 2-4
- Installing wIPS License Files, page 2-9

## Adding a Mobility Services Engine to WCS

To add a mobility services engine to WCS, log in to WCS and follow these steps:

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

**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**, and 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 WCS communication username and password created during the setup process.

If you did not specify the username and password during the setup process, use the default username and password, which are both *admin*.

**Note** If you changed the username and password during the automatic installation script, enter those values at this step. If you did not change the default password, and username, 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.

**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 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 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

**Note** A mobility services engine can support multiple services.

**Step 12** Click **Save**.

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

# Deleting a Mobility Services Engine from the Cisco WCS

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

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

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

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

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

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

# MSE License Overview

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 ContextAware 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 2-3
- Sample MSE License File, page 2-3
- Revoking and Reusing an MSE License, page 2-4

## MSE License Structure Matrix

Table 2-1 lists the breakup of the licenses between the high-end, low-end, and evaluation licenses for MSE, Location services or ContextAware 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 Infra-structure platform. | 60 days. |
| **Location Service or ContextAware 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 MSE. An Increment license is an additive license. In MSE, the individual service engines are treated as Increment licenses.

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

For more information on the license types, see the *Cisco Wireless Control System Configuration Guide, Release 7.0.x.*

## Revoking and Reusing an MSE License

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

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

When you revoke a license, 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 Wireless Control System Configuration Guide, Release 7.0.x.*

### Revoking an MSE License Using MSE CLI

You can also revoke an MSE license from the MSE CLI manually without using WCS.

To revoke an MSE license follow these steps:

---

**Step 1** Log in to an MSE using CLI.

**Step 2** Navigate to /opt/mse/licensing/

**Step 3** Delete the license file by entering this 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:

```
/etc/init.d/msed restart
```

The MSE license is revoked.

---

# Registering Client and wIPS Product Authorization Keys

You receive a product authorization key (PAK) when you order a client, wIPS or tag license from Cisco. You must register the PAK to receive the license file for install on the mobility services engine. License files are e-mailed to you after successfully registering a PAK.

Client and wIPS PAKs are registered with Cisco.

**Note** Tag PAKs are registered with AeroScout only if Aeroscout engine for tags was selected during the Addition of MSE. This procedure is not necessary if Cisco tag engine was selected as the Cisco license will be shared between all devices including the tags. For more information, see the *Cisco Context-Aware Service Configuration Guide* at the following URL: http://www.cisco.com/en/US/products/ps9806/products_installation_and_configuration_guides_list.html

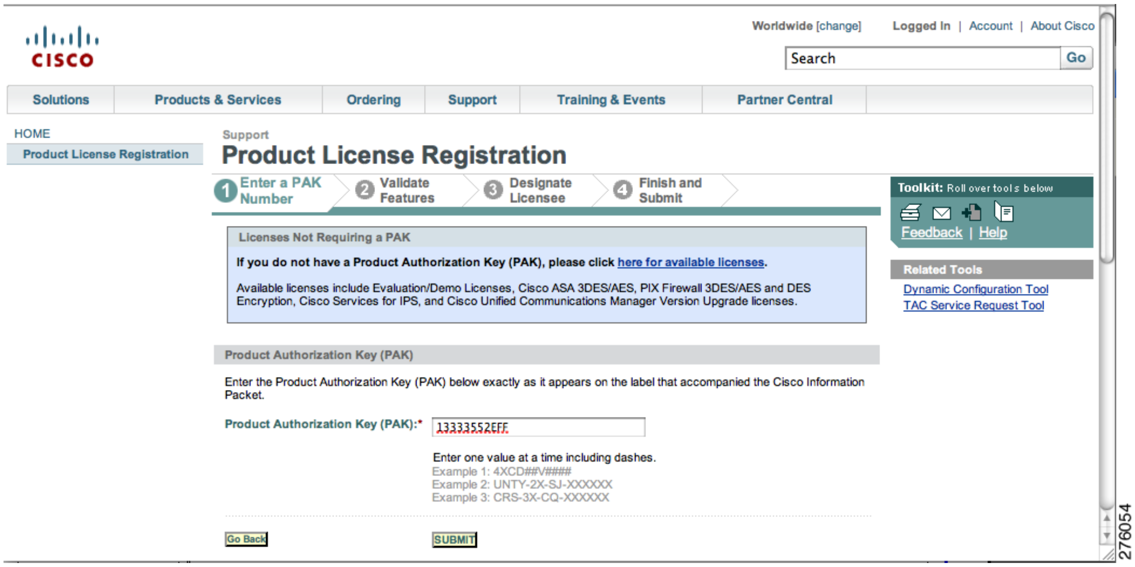
To register a PAK to obtain a license file for installation, follow these steps:

**Step 1** Open a browser window and enter the following URL:

http://www.cisco.com/go/license

**Step 2** Enter the PAK, and click **SUBMIT** (see Figure 2-1).

***Figure 2-1 Enter PAK Number Page***



Licenses Not Requiring a PAK

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

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

Product Authorization Key (PAK)

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

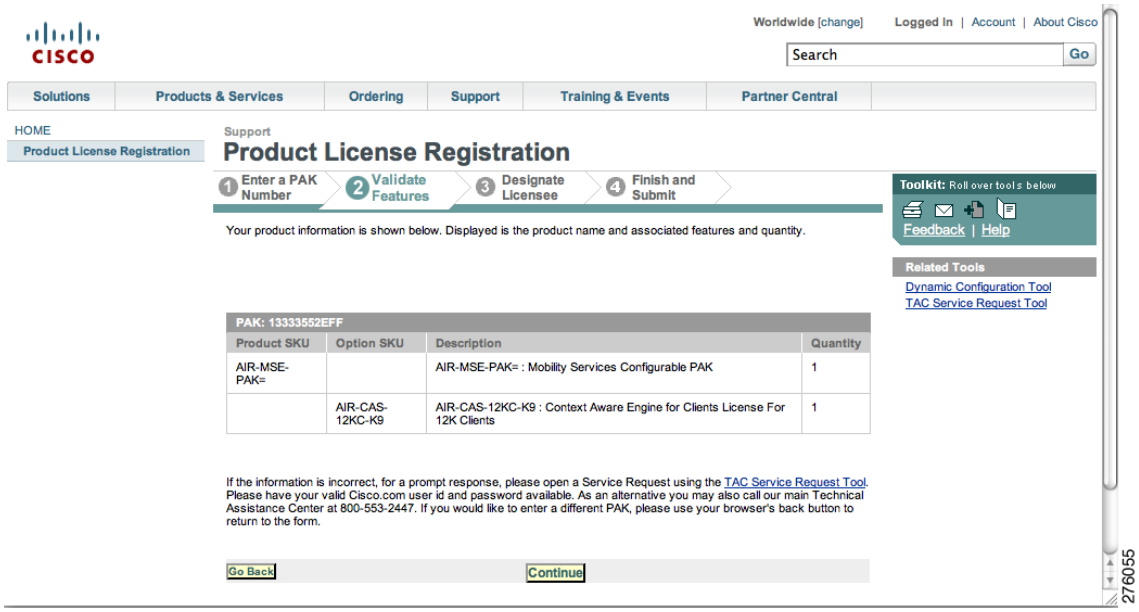
Product Authorization Key (PAK):* 13333552EFF

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

**Step 3** Verify the license purchase. Click **Continue** if the license information is 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** link to report the problem.

*Figure 2-2 Validate Features Page*



Support

Product License Registration

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

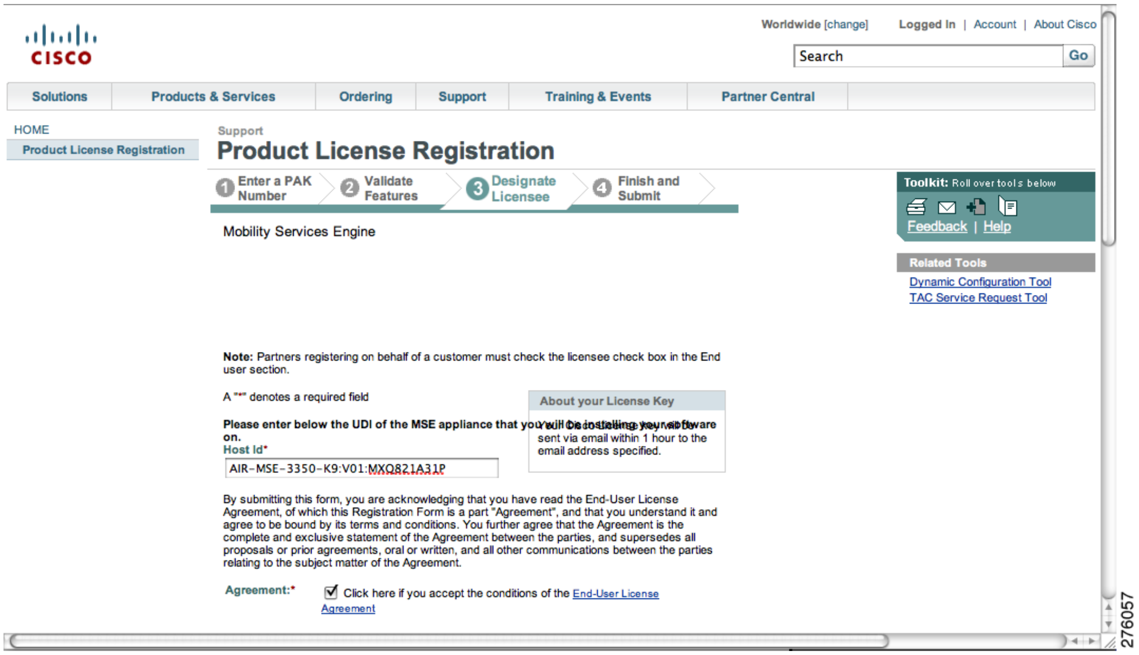
Your product information is shown below. Displayed is the product name and associated features and quantity.

PAK: 13333552EFF

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

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

*Figure 2-3 Designate Licensee, Page 1 of 2*



Support

Product License Registration

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

Mobility Services Engine

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

A "*" denotes a required field

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

Host Id*

AIR-MSE-3350-K9:V01:MXQ821A31P

About your License Key

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

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

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

**Step 4** In the Designate Licensee page:

**a.** Enter the UDI of the mobility services engine in the host id text box. This is the mobility services engine on which the license will be installed.

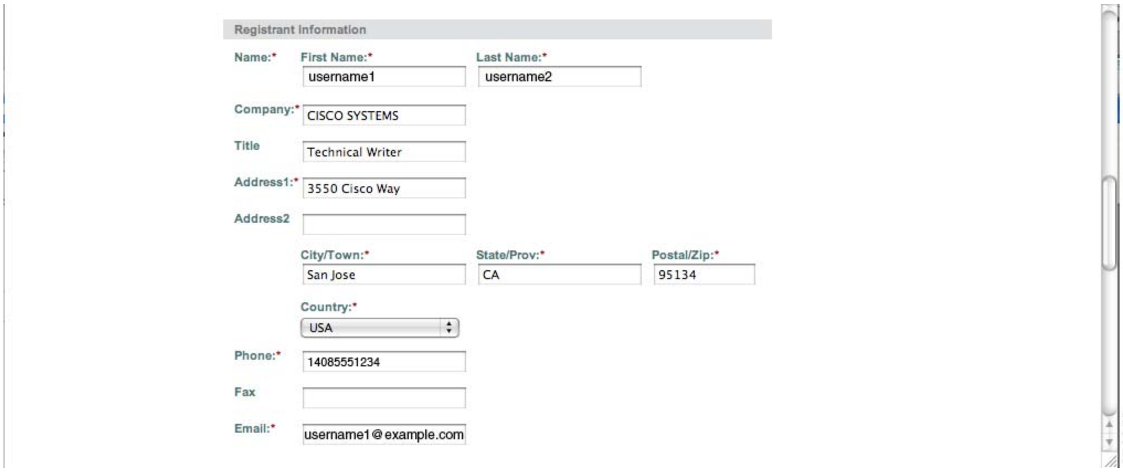
**Note** UDI information for a mobility services engine is found on the General Properties page at Services > Mobility Services Engine > *Device Name* > *System*.

b. Select the **Agreement** check box. Registrant information appears next to the Agreement check box (see Figure 2-4).

Modify the information as necessary.

**Note** Ensure that the phone number for the registrant and end user does not include any characters in the string. For example, enter 555 1212 rather than 555.1212 or 555-1212.

***Figure 2-4 Designate Licensee Page, 2 of 2***



Registrant Information

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

Company:* CISCO SYSTEMS

Title Technical Writer

Address1:* 3550 Cisco Way

Address2

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

Country:* USA

Phone:* 14085551234

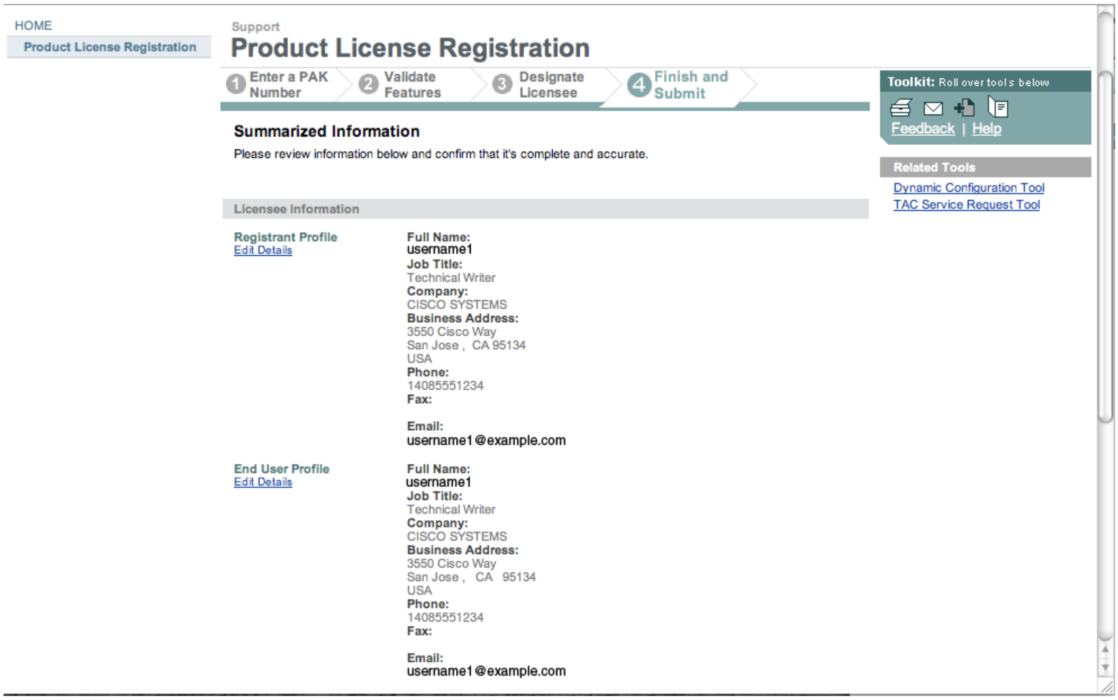
Fax

Email:* username1@example.com

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

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

*Figure 2-5 Finish and Submit Page*



**Summarized Information**

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

Registrant Profile

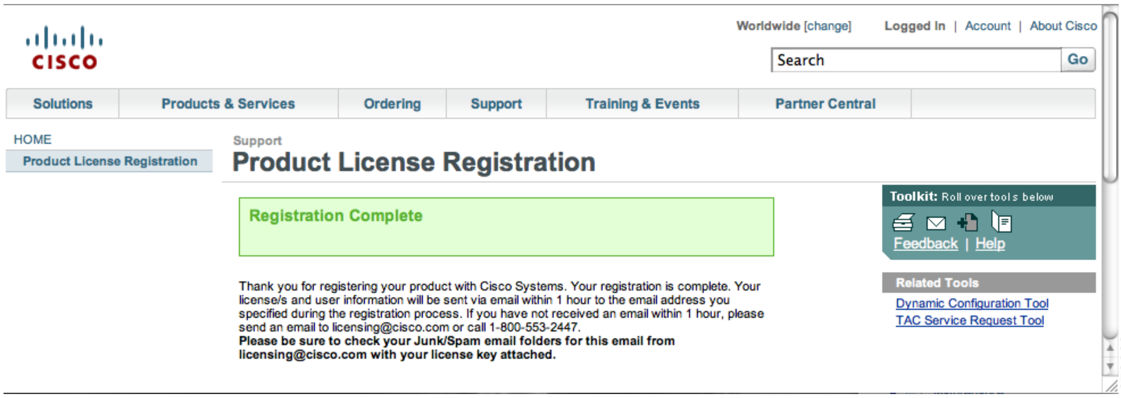
**Full Name:** username1
**Job Title:** Technical Writer
**Company:** CISCO SYSTEMS
**Business Address:** 3550 Cisco Way
San Jose , CA 95134
USA
**Phone:** 14085551234
**Fax:**
**Email:** username1@example.com

End User Profile

**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

**Step 5** In the Finish and Submit page, review registrant and end user data. Click **Edit Details** to correct information. Click **Submit**. A confirmation page appears (see Figure 2-6).

*Figure 2-6 Registration Confirmation Page*



Registration Complete

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

# Installing wIPS License Files

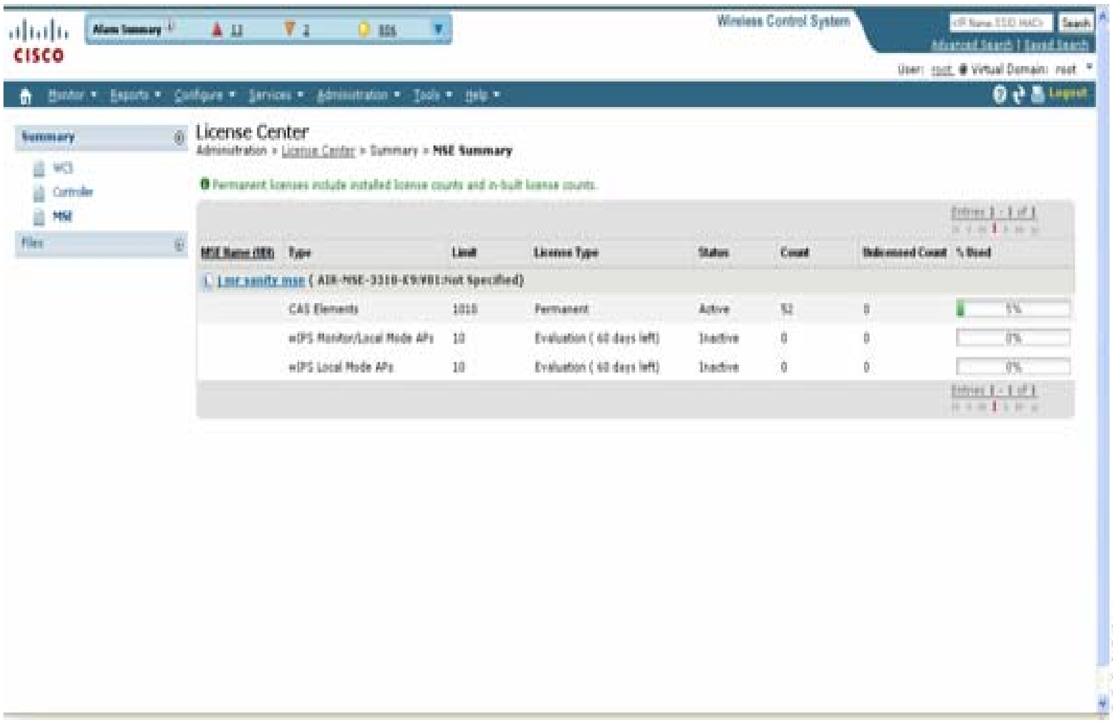
You can install client and wIPS licenses from WCS.

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

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

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

***Figure 2-7 Administration > License Center Page***



License Center

Administration > License Center > Summary > MSE Summary

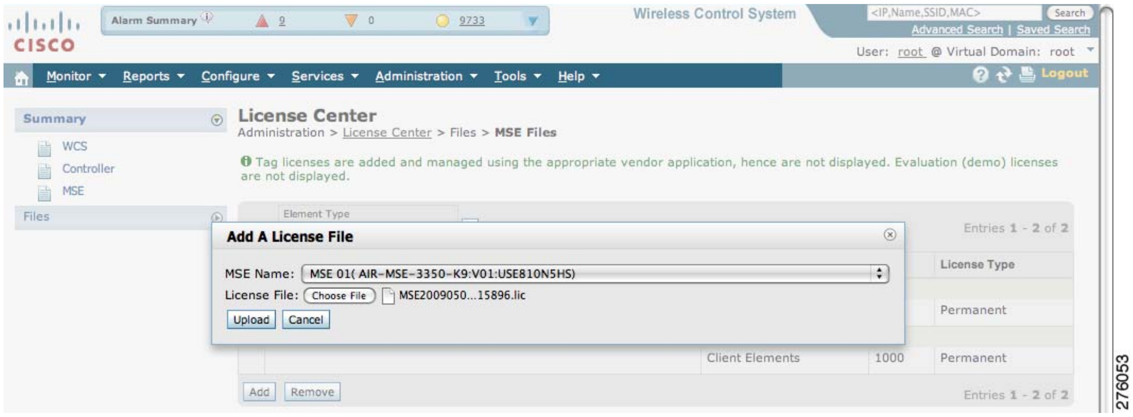
Permanent licenses include installed license counts and in-built license counts.

| MSE Name (IP) | Type | Limit | License Type | Status | Count | Unlicensed Count | % Used |
|---|---|---|---|---|---|---|---|
| Lmr sanity mse ( AIR-MSE-3310-K9:V01:Not Specified) | | | | | | | |
| | CAS Elements | 1010 | Permanent | Active | 52 | 0 | 5% |
| | wIPS Monitor/Local Mode APs | 10 | Evaluation ( 60 days left) | Inactive | 0 | 0 | 0% |
| | wIPS Local Mode APs | 10 | Evaluation ( 60 days left) | Inactive | 0 | 0 | 0% |

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

**Step 3** Click **Add**. The Add a License File dialog box appears (see Figure 2-8).

*Figure 2-8 Add a License File Dialog Box*



License Center

Administration > License Center > Files > MSE Files

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

**Add A License File**

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

License File: MSE2009050...15896.lic

**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 select the license file.

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

CHAPTER 3

# Synchronizing Mobility Services Engines

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

This chapter contains the following sections:

- Synchronizing WCS and Mobility Services Engines, page 3-1
- Viewing Synchronization Information, page 3-7

## Synchronizing WCS and Mobility Services Engines

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

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

- Network Design—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: 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 about third-party application-created event groups, see "Working with Third-Party Elements" section on page 3-5.

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

**Note** Communication between the mobility services engine, WCS and the controller takes place in Coordinated Universal Time (UTC). Moreover, ensure the MSE timezone is set to UTC. Configuring NTP on each system provides devices with the UTC time. The mobility services engine and its associated controllers must be mapped to the same NTP server and the same WCS server. An NTP server is required to automatically synchronize time between the controller, WCS, and the mobility services engine. However, the timezone for MSE should still be set to UTC. This is because wIPS alarms requires that the MSE time be set to UTC.

To synchronize network designs, a controller, a Catalyst switch, or event group with the mobility services engine, follow these steps:

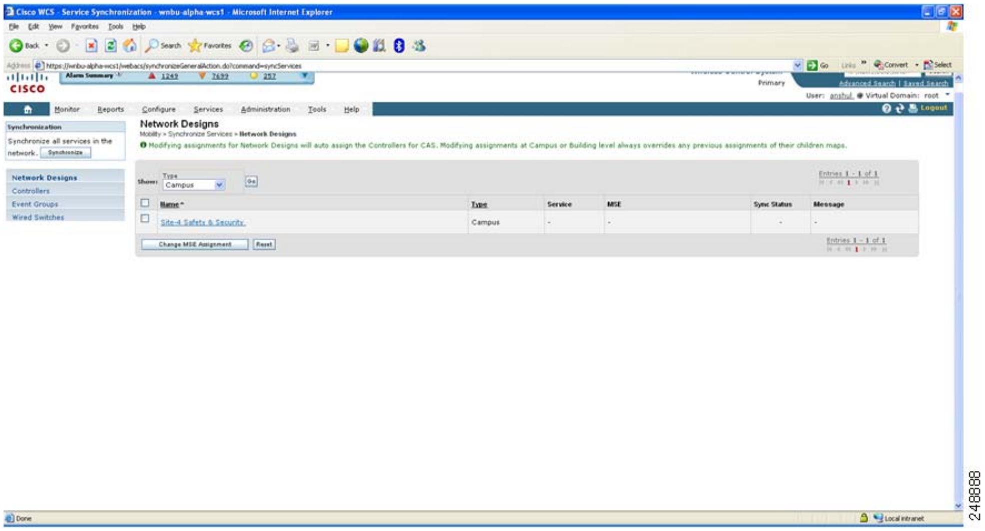
**Step 1** Choose **Services > Synchronize Services**.

The left sidebar menu contains the following options:

- Network Designs
- Controllers
- Event Groups
- Wired Switches

**Step 2** Choose the appropriate menu option (network designs, controllers, event groups, or wired switches). See, Figure 3-1 for more information.

***Figure 3-1 Mobility > Synchronize Services > Network Designs***



Cisco WCS - Service Synchronization - wnbu-alpha-wcs1 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://wnbu-alpha-wcs1/webacs/synchronizeGeneralAction.do?command=syncServices
Go Links Convert Select
CISCO
Alarm Summary 1249 7699 257
Primary
Advanced Search | Saved Search
User: anshul Virtual Domain: root
Monitor Reports Configure Services Administration Tools Help
Logout
Synchronization
Network Designs
Controllers
Event Groups
Wired Switches
Done
Local intranet
248888

Synchronize all services in the network. Synchronize

Network Designs

Mobility > Synchronize Services > Network Designs

Modifying assignments for Network Designs will auto assign the Controllers for CAS. Modifying assignments at Campus or Building level always overrides any previous assignments of their children maps.

Show: Type Campus Go

Entries 1 - 1 of 1

| □ | Name | Type | Service | MSE | Sync Status | Message |
|---|---|---|---|---|---|---|
| □ | Site-4 Safety & Security | Campus | - | - | - | - |

Change MSE Assignment Reset

Entries 1 - 1 of 1

**Step 3** To assign a network design to a mobility services engine, in the synchronization page, choose **Network Designs** from the left sidebar menu.

**Step 4** Choose all the maps to be synchronized with the mobility services engine.

> **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. See, Figure 3-2 for more information.

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

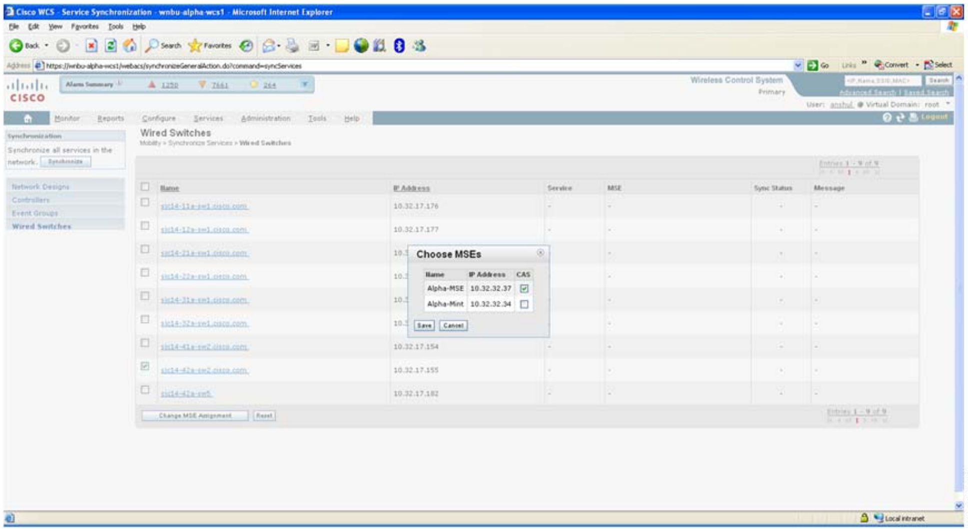
- Save—Saves the mobility services engine assignment. The following message appears in the Messages column of the Network Designs page with yellow arrows icon:

  **`To be assigned - Please synchronize`**.

- Cancel—Discards the changes to mobility services engine assignment and returns to the Network Designs page.

You can also select one or more maps and click **Reset** to undo the assignments for those maps.

***Figure 3-2 MSE Assignment Page***



Cisco WCS - Service Synchronization - wnbu-alpha-wcs1 - Microsoft Internet Explorer
https://wnbu-alpha-wcs1/webacs/synchronizeGeneralAction.do?command=syncServices
Wireless Control System
Primary
Monitor
Reports
Configure
Services
Administration
Tools
Help
Synchronization
Synchronize all services in the network.
Synchronize
Network Designs
Controllers
Event Groups
Wired Switches
Change MSE Assignment
Reset
248887

Wired Switches

Mobility > Synchronize Services > Wired Switches

Entries 1 - 9 of 9

| □ | Name | IP Address | Service | MSE | Sync Status | Message |
|---|---|---|---|---|---|---|
| □ | sjc14-11a-sw1.cisco.com | 10.32.17.176 | - | - | - | - |
| □ | sjc14-12a-sw1.cisco.com | 10.32.17.177 | - | - | - | - |
| □ | sjc14-21a-sw1.cisco.com | 10.3 | | - | - | - |
| □ | sjc14-22a-sw1.cisco.com | 10.3 | | - | - | - |
| □ | sjc14-31a-sw1.cisco.com | 10.3 | | - | - | - |
| □ | sjc14-32a-sw1.cisco.com | 10.3 | | - | - | - |
| □ | sjc14-41a-sw2.cisco.com | 10.32.17.154 | - | - | - | - |
| ☑ | sjc14-42a-sw2.cisco.com | 10.32.17.155 | - | - | - | - |
| □ | sjc14-42a-sw5. | 10.32.17.182 | - | - | - | - |

Choose MSEs

| Name | IP Address | CAS |
|---|---|---|
| Alpha-MSE | 10.32.32.37 | ☑ |
| Alpha-Mint | 10.32.32.34 | □ |

Save Cancel

> **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, page 3-4 for more information.

## Synchronizing Controllers with a Mobility Services Engine

You can assign an MSE to any wireless controller on a per-service (wIPS) basis.

To associate a mobility services engine with a controller, follow these steps:

**Step 1** In the synchronization page, choose **Controllers** from the left sidebar menu.

**Step 2** Choose the controllers to be assigned to the mobility services engine.

**Step 3** Click **Change MSE Assignment**.

**Step 4** Choose the mobility services engine to which the controllers must be synchronized.

**Step 5** Click either of the following in the popup window:

- OK—Saves the mobility services engine assignment. The following message appears in the Messages column of the Controllers page with yellow arrows icon:

  ```
  To be assigned - Please synchronize.
  ```

- Cancel—Discards the changes to mobility services engine assignment and returns to the Controllers page.

You can also select one or more controllers and click **Reset** to undo the assignments for those controllers.

**Step 6** Click **Synchronize** to complete the synchronization process.

**Step 7** Confirm 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.
- Controller names must be unique for synchronizing with a mobility services engine. If you have two controllers with the same name, only one will be 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.

To unassign a network design, controller, event group, or wired switch from a mobility services engine follow these steps:

**Step 1** On the respective tabs, choose one or more elements and click **Change MSE Assignment**. The choose mobility services engine dialog box appears.

**Step 2** Unselect the mobility services engine if you do not want the elements to be associated with that mobility services engine.

**Step 3** Click **Save** to save the changes to the assignments.

**Step 4** Click **Synchronize**. A two-arrow icon appears in the Sync Status column.

## Working with Third-Party Elements

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

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

**Step 1** In the Synchronization page, choose **Third-Party Elements** from the left sidebar menu.

The Third-Party Elements page appears.

**Step 2** Select one or more elements.

**Step 3** Click one of the following buttons:

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

## Configuring Automatic Database Synchronization and Out-of-Sync Alerts

Manual synchronization of the WCS 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 WCS to carry out synchronization. This policy ensures that synchronization between WCS and mobility services engine databases is triggered periodically and any related alarms are cleared.

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

To further ensure that WCS and MSE are in sync, smart synchronization happens in the background. To configure smart synchronization, follow these steps:

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

**Step 2** Select the **Mobility Service Synchronization** check box.

**Step 3** Click the **Mobility Service Synchronization** link.

The Task > Mobility Service Synchronization page appears.

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

**Step 5** To enable smart synchronization, select the Smart Synchronization **Enabled** check box.

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

**Note** When a mobility services engine is added to a WCS, the data in the WCS 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 WCS, are removed automatically from the mobility services engine.

**Step 6** Enter the time interval in days and the time of day (xx:yy AM or PM) that the automatic synchronization is to be performed.

By default, smart-sync is enabled.

**Step 7** Click **Submit**.

For smart controller assignment and selection scenarios, see Smart Controller Assignment and Selection Scenarios.

## Smart Controller Assignment and Selection Scenarios

**Scenario 1**

If a floor having at least one access point from a controller is chosen to be synchronized with the mobility services engine in the Network Designs section of the Synchronization page, then the controller to which that access point is connected is automatically selected to be assigned to the mobility services engine for CAS service.

**Scenario 2**

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

**Scenario 3**

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

**Scenario 4**

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

## Out-of-Sync Alarms

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

- Elements are modified in WCS (the auto-sync policy pushes these elements)
- Elements other than controllers exist in the mobility services engine database but not in WCS
- 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 alarms for the elements not assigned to any server will also be deleted.

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

# Viewing Synchronization Information

This section describes how to view synchronization status and history and contains the following topics:

- Viewing Mobility Services Engine Synchronization Status, page 3-7
- Viewing Synchronization History, page 3-8

## Viewing Mobility Services Engine Synchronization Status

You can use the Synchronize Services feature in WCS to view the status of network design, controller, switch, and event group synchronization with a mobility services engine.

To view synchronization status, follow these steps:

**Step 1** In WCS, choose **Services > Synchronize Services**.

**Step 2** From the left sidebar menu, choose the applicable option (Network Designs, Controllers, Event Groups, or Wired Switches).

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

You can also view the synchronization status and assign or unassign from campus view and building view along with floor view.

To access this page, choose **Monitor > Maps > System Campus >** ***Building*** **>** ***Floor***

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

On the left sidebar menu, there is an option MSE Assignment. This option shows which mobility services engine the floor is currently assigned to. You can also change mobility services engine assignment in this page.

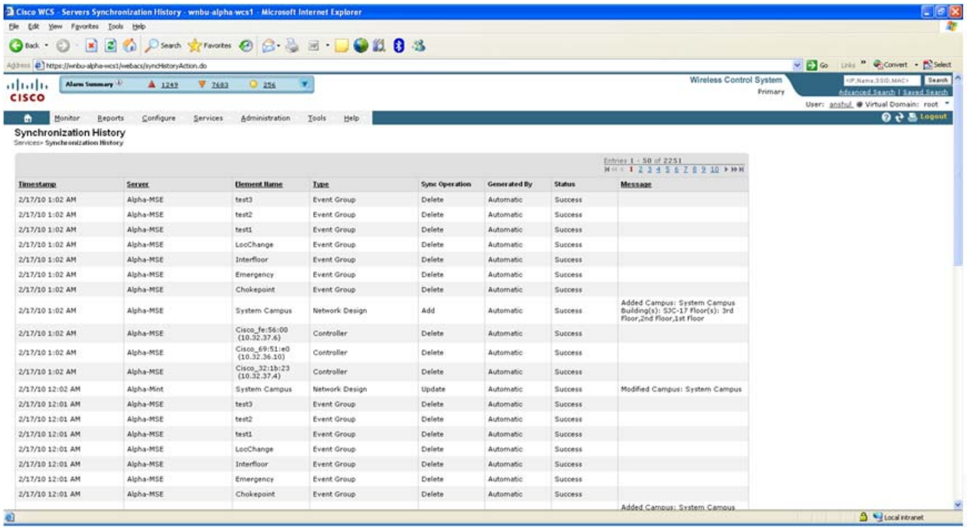
# Viewing Synchronization History

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, follow these steps:

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

***Figure 3-3 Mobility > Synchronization History***


Cisco WCS - Servers Synchronization History - wnbu-alpha-wcs1 - Microsoft Internet Explorer
https://wnbu-alpha-wcs1/webacs/syncHistoryAction.do
Alarm Summary
1249
7683
256
Wireless Control System
Monitor
Reports
Configure
Services
Administration
Tools
Help

Synchronization History
Services > Synchronization History

Entries 1 - 50 of 2251

| Timestamp | Server | Element Name | Type | Sync Operation | Generated By | Status | Message |
|---|---|---|---|---|---|---|---|
| 2/17/10 1:02 AM | Alpha-MSE | test3 | Event Group | Delete | Automatic | Success | |
| 2/17/10 1:02 AM | Alpha-MSE | test2 | Event Group | Delete | Automatic | Success | |
| 2/17/10 1:02 AM | Alpha-MSE | test1 | Event Group | Delete | Automatic | Success | |
| 2/17/10 1:02 AM | Alpha-MSE | LocChange | Event Group | Delete | Automatic | Success | |
| 2/17/10 1:02 AM | Alpha-MSE | Interfloor | Event Group | Delete | Automatic | Success | |
| 2/17/10 1:02 AM | Alpha-MSE | Emergency | Event Group | Delete | Automatic | Success | |
| 2/17/10 1:02 AM | Alpha-MSE | Chokepoint | Event Group | Delete | Automatic | Success | |
| 2/17/10 1:02 AM | Alpha-MSE | System Campus | Network Design | Add | Automatic | Success | Added Campus: System Campus Building(s): SJC-17 Floor(s): 3rd Floor,2nd Floor,1st Floor |
| 2/17/10 1:02 AM | Alpha-MSE | Cisco_fe:56:00 (10.32.37.6) | Controller | Delete | Automatic | Success | |
| 2/17/10 1:02 AM | Alpha-MSE | Cisco_69:51:e0 (10.32.36.10) | Controller | Delete | Automatic | Success | |
| 2/17/10 1:02 AM | Alpha-MSE | Cisco_32:1b:23 (10.32.37.4) | Controller | Delete | Automatic | Success | |
| 2/17/10 12:02 AM | Alpha-Mint | System Campus | Network Design | Update | Automatic | Success | Modified Campus: System Campus |
| 2/17/10 12:01 AM | Alpha-MSE | test3 | Event Group | Delete | Automatic | Success | |
| 2/17/10 12:01 AM | Alpha-MSE | test2 | Event Group | Delete | Automatic | Success | |
| 2/17/10 12:01 AM | Alpha-MSE | test1 | Event Group | Delete | Automatic | Success | |
| 2/17/10 12:01 AM | Alpha-MSE | LocChange | Event Group | Delete | Automatic | Success | |
| 2/17/10 12:01 AM | Alpha-MSE | Interfloor | Event Group | Delete | Automatic | Success | |
| 2/17/10 12:01 AM | Alpha-MSE | Emergency | Event Group | Delete | Automatic | Success | |
| 2/17/10 12:01 AM | Alpha-MSE | Chokepoint | Event Group | Delete | Automatic | Success | |
| | | | | | | | Added Campus: System Campus |

248889

**Step 2** Table 3-1 describes the text boxes that appear in the Synchronization History page.

*Table 3-1 Synchronization History*

| Text Box | Description |
|---|---|
| Timestamp | The date and time at which the synchronization has happened. |
| Server | The mobility services engine server. |
| Element Name | The name of the element that was synchronized. |
| Type | The type of the element that was synchronized. |
| Sync Operation | The sync operation that was performed.<br>Either be Update or Add. |
| Generated By | The method of synchronization.<br>Either be Manual or Automatic. |
| Status | The status of the synchronization. It can be Either Success or Failed. |
| Message | Any additional message about the synchronization. |

Click the column headers to sort the entries.

CHAPTER 4

# Configuring and Viewing System Properties

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

This chapter contains the following sections:

- Editing General Properties and Viewing Performance, page 4-1
- Modifying NMSP Parameters, page 4-5
- Viewing Active Sessions on a System, page 4-7
- Adding and Deleting Trap Destinations, page 4-7
- Viewing and Configuring Advanced Parameters, page 4-9

# Editing General Properties and Viewing Performance

General Properties—You can use Cisco WCS to edit the general properties of a mobility services engine such as contact name, username, password, services enabled on the system, enabling or disabling a service or enabling the mobility services engine for synchronization. Refer to the "Editing General Properties" section on page 4-1.

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

This section contains the following topics:

- Editing General Properties, page 4-1
- Viewing Performance Information, page 4-4

## Editing General Properties

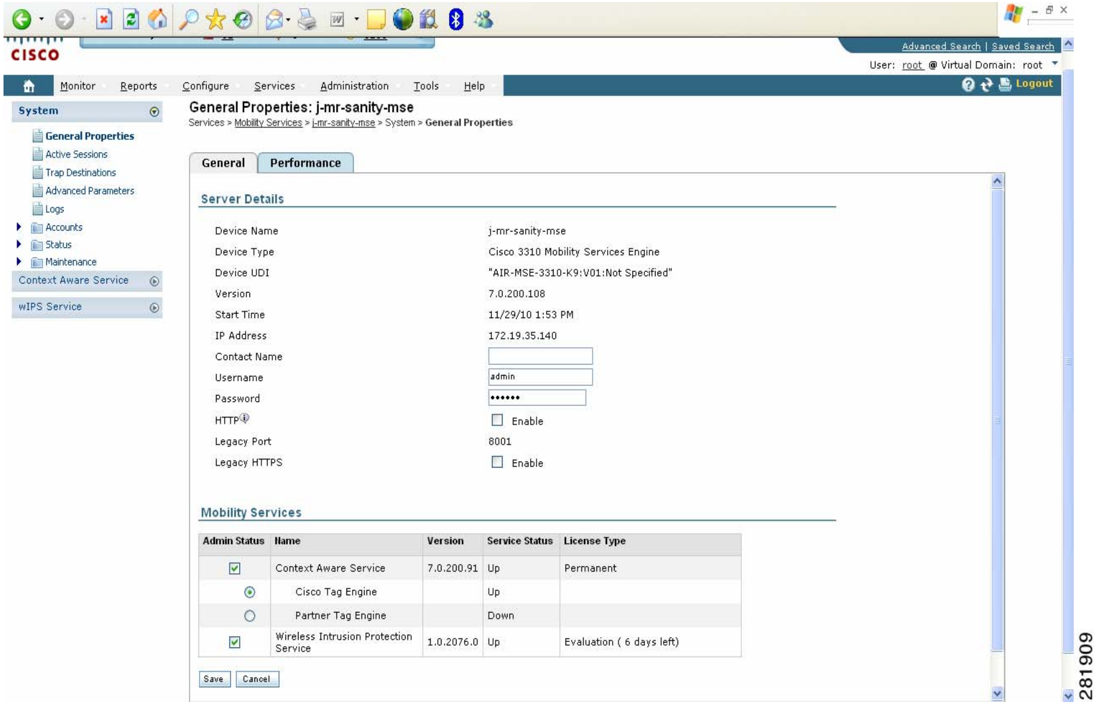
To edit the general properties of a mobility services engine, follow these steps:

**Step 1** In WCS, choose **Services > Mobility Services** 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 (see Figure 4-1).

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

*Figure 4-1 General Properties*



General Properties: j-mr-sanity-mse

Services > Mobility Services > j-mr-sanity-mse > System > General Properties

Server Details

| | |
|---|---|
| Device Name | j-mr-sanity-mse |
| Device Type | Cisco 3310 Mobility Services Engine |
| Device UDI | "AIR-MSE-3310-K9:V01:Not Specified" |
| Version | 7.0.200.108 |
| Start Time | 11/29/10 1:53 PM |
| IP Address | 172.19.35.140 |
| Contact Name | |
| Username | admin |
| Password | •••••• |
| HTTP | □ Enable |
| Legacy Port | 8001 |
| Legacy HTTPS | □ Enable |

Mobility Services

| Admin Status | Name | Version | Service Status | License Type |
|---|---|---|---|---|
| ☑ | Context Aware Service | 7.0.200.91 | Up | Permanent |
| ● | Cisco Tag Engine | | Up | |
| ○ | Partner Tag Engine | | Down | |
| ☑ | Wireless Intrusion Protection Service | 1.0.2076.0 | Up | Evaluation ( 6 days left) |

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

*Table 4-1 General Properties*

| Parameter | Configuration Options |
|---|---|
| Contact Name | Enter a contact name for the mobility services engine. |
| User Name | Enter the login username for the WCS server that manages the mobility services engine. |
| Password | Enter the login password for the WCS server that manages the mobility services engine. |
| HTTP | Select the **Enable** check box to enable HTTP. By default, HTTPS is enabled.<br>**Note** HTTP is primarily enabled to allow third-party applications to communicate with the mobility services engine.<br>**Note** WCS always communicates through HTTPS. |
| Legacy Port | Enter the mobility services port number that supports HTTPS communication. The Legacy HTTPS option must also be enabled. Default value is 8001. |
| Legacy HTTPS | This parameter does not apply to mobility services engines. It applies only to location appliances. |

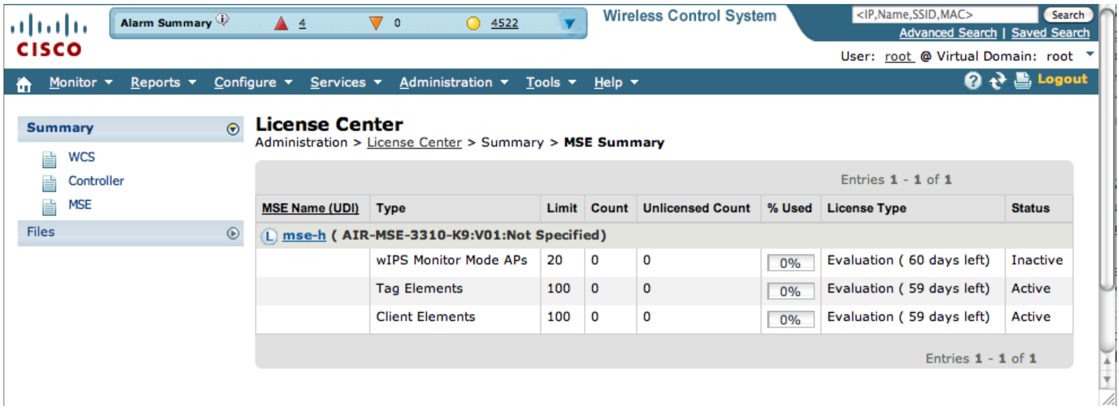
*Table 4-1 General Properties (continued)*

| Parameter | Configuration Options |
|---|---|
| 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 will show up only when the delete synchronized service assignments check box was unselected while adding an mobility services engine. |
| Mobility Services | To enable a service on the mobility services engine, select the check box next to the service. Services include Context Aware and wIPS.<br>You can choose CAS to track clients, rogues, interferers, wired clients, and tags.<br>Choose either of the following engines to track tags:<br>• Cisco Tag Engine<br>or<br>• Partner Tag Engine<br>**Note** Once selected, the service displays as Up (active). All inactive services are noted as Down (inactive) on the selected (current) system and on the network.<br>**Note** CAS and wIPS can operate on a mobility services engine at the same time.<br>**Note** All mobility services engines are shipped with an evaluation license of CAS and wIPS. Evaluation copies are good for a period of 60 days (480 hours) and have preset device limits for each service. Licenses are usage-based (time is decremented by the number of days you use it rather than by the number of calendar days passed).<br>Click the **here** link to see the number of devices that can be assigned for the current system (see Figure 4-1).<br>In the License Center page (see Figure 4-2), choose the **MSE** left sidebar menu option to see license details for all mobility services engines on the network (see Figure 4-3).<br>**Note** For more information on purchasing and installing licenses, refer to:<br>http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html |

**Note** The following TCP ports are in use on an MSE in Release 6.0 and above: 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 an MSE in Release 6.0 and above: 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.

***Figure 4-2 License Summary for Selected Mobility Services Engine***



License Center

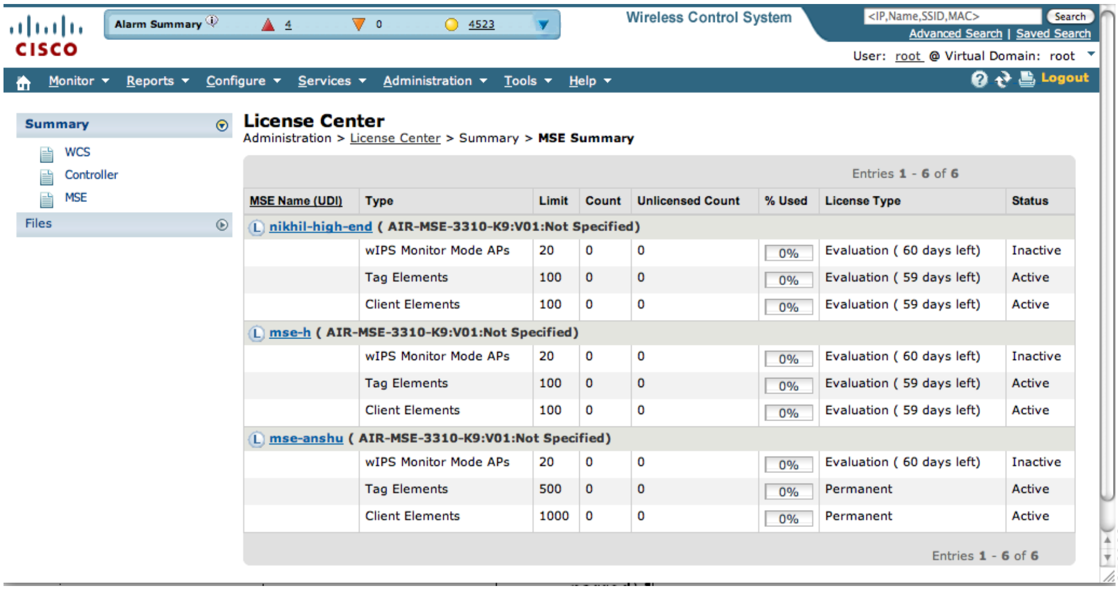
Administration > License Center > Summary > **MSE Summary**

Entries 1 - 1 of 1

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

Entries 1 - 1 of 1

***Figure 4-3 License Summary for All Mobility Services Engines***



License Center

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

Entries 1 - 6 of 6

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

Entries 1 - 6 of 6

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

# Viewing Performance Information

To view performance details, follow these steps:

**Step 1** In WCS, 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.

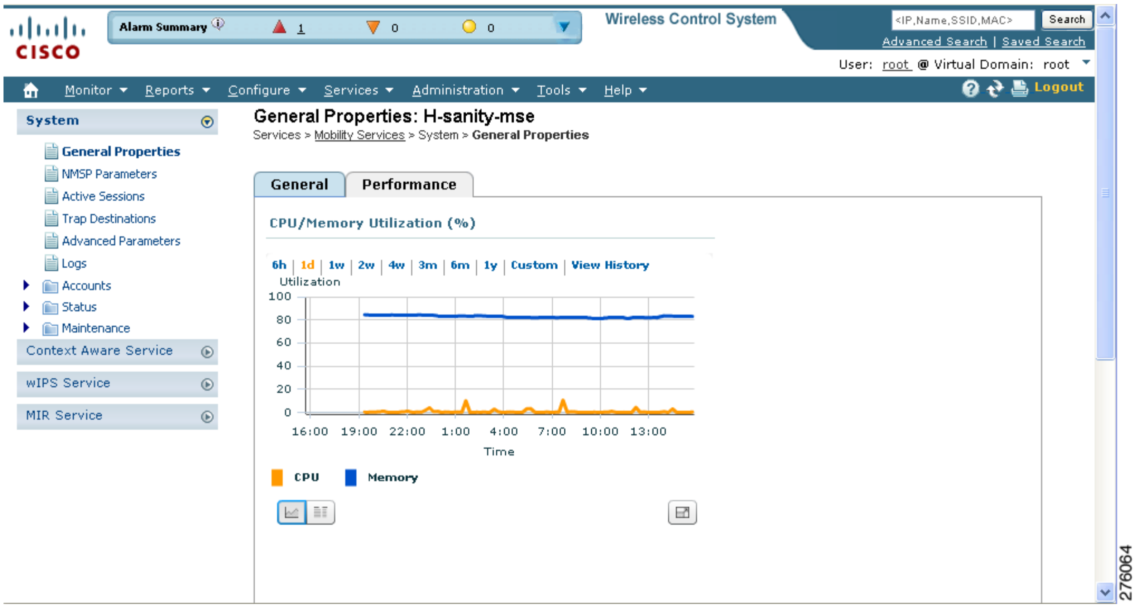
**Step 3** Click the **Performance** tab (see Figure 4-4).

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

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

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

***Figure 4-4 CPU and Memory Performance***



# Modifying NMSP Parameters

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

**Note** This menu option is only available in MSE releases prior to 7.0.105.0.

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

**Note** Telemetry, emergency, and chokepoint information is only seen on controllers and WCS installed with Release 4.1 software or later.

**Note** The TCP port (16113) that the controller or Catalyst switch and the mobility services engine communicate over *must* be open (not blocked) on any firewall that exists between the controller or Catalyst switch and mobility services engine for NMSP to function.

To configure NMSP parameters, follow these steps:

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

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

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

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

*Table 4-2 NMSP Parameters*

| Parameter | Description |
|---|---|
| Echo Interval | How frequently an echo request is sent from a mobility services engine to a controller. The default value is 15 seconds. Allowed values range from 1 to 120 seconds.<br>**Note** If a network is experiencing slow response, you can increase the values of the echo interval, neighbor dead interval and the response timeout values to limit the number of failed echo acknowledgements. |
| Neighbor Dead Interval | The number of seconds that the mobility services engine waits for a successful echo response from the controller before declaring the neighbor dead. This timer begins when the echo request is sent.<br>The default values is 30 seconds. Allowed values range from 1 to 240 seconds.<br>**Note** This value must be at least two times the echo interval value. |
| Response Timeout | How long the mobility services engine waits before considering the pending request as timed out. The default value is 1 second. Minimum value is one (1). There is no maximum value. |
| Retransmit Interval | Interval of time that the mobility services engine waits between notification of a response time out and initiation of a request retransmission. The default setting is 3 seconds. Allowed values range from 1 to 120 seconds. |
| Maximum Retransmits | The maximum number of retransmits that are sent in the absence of a response to any request. The default setting is 5. Allowed minimum value is zero (0). There is no maximum value. |

**Step 5** Click **Save** to update the Cisco WCS and mobility services engine databases.

# Viewing Active Sessions on a System

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

For every session, WCS displays the following information:

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

To view active user sessions, follow these steps:

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

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

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

# Adding and Deleting Trap Destinations

You can specify which WCS or Cisco Security Monitoring, Analysis, and Response System (CS-MARS) network management platform is the recipient of SNMP traps generated by the mobility services engine.

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

This section contains the following topics:

- Adding Trap Destinations, page 4-7
- Deleting Trap Destinations, page 4-8

## Adding Trap Destinations

To add a trap destination, follow these steps:

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

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

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

**Step 4** From the Select a command drop-down list, choose **Add Trap Destination**, and click **Go**.

The Add Trap Destination page appears.

**Step 5** Table 4-3 lists the various fields in the New Trap Destination page.

*Table 4-3 Add Trap Destination*

| Field | Description |
|---|---|
| IP Address | IP address for the trap destination. |
| Port Number | Port number for the trap destination. The default port number is 162. |
| Destination Type | This field is not editable and has a value **Other**. |
| SNMP Version | Select either v2c or v3. |
| The following fields appear only if you select v3 as the SNMP version: | |
| User Name | Username for the SNMP version 3. |
| Security Name | Security name for the SNMP version 3. |
| Authentication Type | Select either of the following:<br>HMAC-MD5<br>HMAC-SHA |
| Authentication Password | Authentication password for the SNMP version 3. |
| Privacy Type | Select either of the following:<br>CBC-DES<br>CFB-AES-128<br>CFB-AES-192<br>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 6** Click **Save**.

You are returned to the Trap Destinations summary page and the newly defined trap is listed.

# Deleting Trap Destinations

To delete a trap destination, follow these steps;

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

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

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

**Step 4** 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 **Delete Trap Destination**, and click **Go**.

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

# Viewing and Configuring Advanced Parameters

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

- Refer to the "Viewing Advanced Parameters Settings" section on page 4-9 to view current system-level advanced parameters.
- Refer to the "Initiating Advanced Commands" section on page 4-11 to modify the current system-level advanced parameters or initiate advanced commands such as system reboot, system shutdown, or clear a configuration file.

This section contains the following topics:

- Viewing Advanced Parameters Settings, page 4-9
- Initiating Advanced Parameters, page 4-10
- Initiating Advanced Commands, page 4-11

## Viewing Advanced Parameters Settings

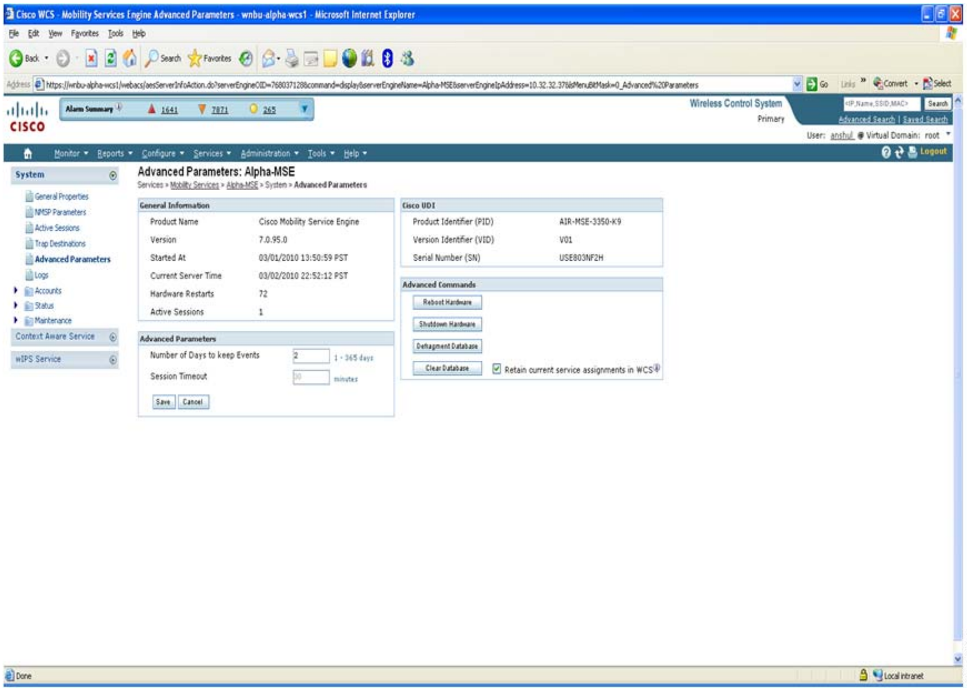
To view the advanced parameter settings of the mobility services engine, follow these steps:

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

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

**Step 3** Choose **System** > **Advanced Parameters** (see Figure 4-5).

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



Cisco WCS - Mobility Services Engine Advanced Parameters - wnbu-alpha-wcs1 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Alarm Summary 1641 7871 265
Wireless Control System
Monitor Reports Configure Services Administration Tools Help
Logout
System
General Properties
NMSP Parameters
Active Sessions
Trap Destinations
Advanced Parameters
Logs
Accounts
Status
Maintenance
Context Aware Service
wIPS Service
Done
Local intranet
248911

Address https://wnbu-alpha-wcs1/webacs/aesServerInfoAction.do?serverEngineOID=768037128&command=display&serverEngineName=Alpha-MSE&serverEngineIpAddress=10.32.32.37&leftMenuBitMask=0_Advanced%20Parameters

Advanced Parameters: Alpha-MSE

Services > Mobility Services > Alpha-MSE > System > **Advanced Parameters**

**General Information**

| | |
|---|---|
| Product Name | Cisco Mobility Service Engine |
| Version | 7.0.95.0 |
| Started At | 03/01/2010 13:50:59 PST |
| Current Server Time | 03/02/2010 22:52:12 PST |
| Hardware Restarts | 72 |
| Active Sessions | 1 |

**Cisco UDI**

| | |
|---|---|
| Product Identifier (PID) | AIR-MSE-3350-K9 |
| Version Identifier (VID) | V01 |
| Serial Number (SN) | USE803NF2H |

**Advanced Parameters**

Number of Days to keep Events: 2 (1 - 365 days)

Session Timeout: 30 minutes

Save Cancel

**Advanced Commands**

Reboot Hardware

Shutdown Hardware

Defragment Database

Clear Database ☑ Retain current service assignments in WCS

# Initiating Advanced Parameters

The Advanced Parameters section of WCS 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 shutdown, or clear the system database.

**Note** You can use WCS to modify troubleshooting parameters for a mobility services engine or a location appliance.

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

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

  For more information, see Configuring Advanced Parameters, page 4-10.

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

  For more information, see Initiating Advanced Commands, page 4-11.

## Configuring Advanced Parameters

To configure advanced parameters, follow these steps:

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

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

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

**Step 4** View or modify the advanced parameters as necessary.

- General Information
- 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 greyed out.
- 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, page 4-11 for more information.
  - Shutdown Hardware—Click to turn off the mobility services hardware. See Rebooting or Shutting Down a System, page 4-11 for more information.
  - Clear Database—Click to clear the mobility services database. See Clearing the System Database, page 4-12 for more information. Unselect the **Retain current service assignments in WCS** check box to remove all existing services assignments from the WCS and MSE. The resources have to be reassigned in the Services > Synchronize Services page. By default this option is selected.

**Step 5** Click **Save** to update the WCS and mobility services databases.

# Initiating Advanced Commands

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

This section contains the following topics:

- Rebooting or Shutting Down a System, page 4-11
- Clearing the System Database, page 4-12

## Rebooting or Shutting Down a System

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

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

**Step 2** Click the name of a mobility services engine you want to reboot or shut down.

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

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

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

## Clearing the System Database

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

**Step 1** In WCS, click **Services > Mobility Services**.

**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 section, unselect the **Retain current service assignments in WCS** check box to remove all existing service assignments from WCS and MSE.

The resources must be reassigned in the Services > Synchronize Services page. By default, this option is checked.

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

**Step 6** Click **OK** to clear the mobility services engine database.

CHAPTER 5

# Managing Users and Groups

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

This chapter contains the following sections:

- Managing Groups, page 5-1
- Managing Users, page 5-2

## Managing Groups

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

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

**Caution** Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with read access permission, that user will not be able to configure mobility services engine settings.

This section contains the following topics:

- Adding User Groups, page 5-1
- Deleting User Groups, page 5-2
- Changing User Group Permissions, page 5-2

### Adding User Groups

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

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

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

**Step 3** Choose **System > Accounts > Groups**.

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

**Step 5** Enter the name of the group in the Group Name text box.

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

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

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

## Deleting User Groups

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

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

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

**Step 3** Choose **System > Accounts > Groups**.

**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 a user full access and add that user to a group with read access permission, that user will not be able to configure mobility services engine settings.

To change user group permissions, follow these steps:

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

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

**Step 3** Choose **System > Accounts > Groups**.

**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, or full).

**Step 6** Click **Save**.

# Managing Users

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

This section contains the following topics:

Adding Users, page 5-3

Deleting Users, page 5-4

## 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 read access permission, that user will not be able to configure mobility services engine settings.

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

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

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

**Step 3** Choose **System > Accounts > Users**.

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

**Step 5** Enter the username in the Username text box.

**Step 6** Enter a password in the Password text box.

**Step 7** Enter the name of the group to which the user belongs in the Group Name text box.

**Step 8** From the Permission drop-down list, choose a permission level (read, write, or full).

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

**Step 9** Click **Save**.

## Deleting Users

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

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

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

**Step 3** Choose **System > Accounts > Users**.

**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**, and click **Go**.

**Step 6** Click **OK**.

## Changing User Properties

To change user properties, follow these steps:

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

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

**Step 3** Choose **System > Accounts > Users**.

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

**Step 5** Make the required changes to the Password, Group Name, and Permission text boxes.

**Step 6** Click **Save**.

CHAPTER 6

# Configuring wIPS and Profiles

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

This chapter contains the following sections:

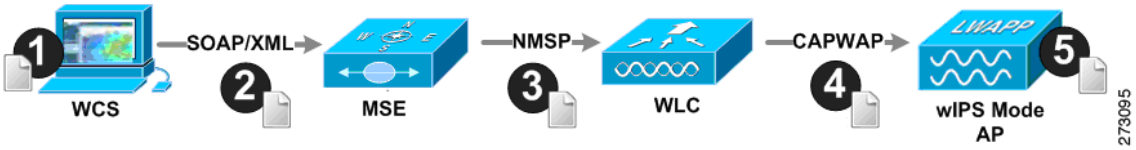
- Configuring Access Points for wIPS Monitor Mode, page 6-2
- Configuring wIPS Profiles, page 6-4

## Overview of wIPS Configuration and Profile Management

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

From the wIPS service on the mobility services engine, profiles are propagated to specific controllers, which in turn communicate this profile transparently to wIPS mode access points associated to that respective controller. (See Figure 6-1).

*Figure 6-1 Configuration and Update of wIPS Profiles*



**Note** If your wIPS deployment consists of a controller, access point, and MSE, you must set all the three entities to the UTC timezone.

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

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

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

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

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

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

1. Install a mobility services engine (if one is not already operating in the network). Refer to the *Cisco 3350 Mobility Services Engine Getting Started Guide* or *Cisco 3310 Mobility Services Engine Getting Started Guide*:

   http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html
2. Add the mobility services engine to WCS (if not already added). See the "Adding and Deleting Systems" section on page 2-1.
3. Configure access points to operate in wIPS monitor mode. See the "Configuring Access Points for wIPS Monitor Mode" section on page 6-2.
4. Configure wIPS profiles. See the "Configuring wIPS Profiles" section on page 6-4.

This section contains the following topics:

- Configuring Access Points for wIPS Monitor Mode, page 6-2
- Configuring wIPS Profiles, page 6-4

# Configuring Access Points for wIPS Monitor Mode

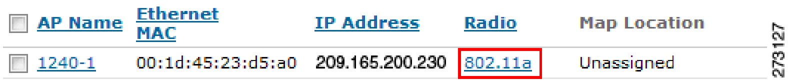
**Note** Only Cisco Aironet 1130, 1140, 1240, and 1250 Series Access Points support wIPS monitor mode.

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

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

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

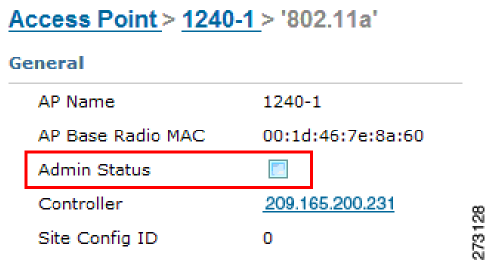
***Figure 6-2 Configure > Access Points > Radio***



| □ | AP Name | Ethernet MAC | IP Address | Radio | Map Location |
|---|---|---|---|---|---|
| □ | 1240-1 | 00:1d:45:23:d5:a0 | 209.165.200.230 | 802.11a | Unassigned |

**Step 3** On the access point page, unselect the **Admin Status** check box to disable the radio.

*Figure 6-3 Access Points > Radio*



Access Point > 1240-1 > '802.11a'

General

| | |
|---|---|
| AP Name | 1240-1 |
| AP Base Radio MAC | 00:1d:46:7e:8a:60 |
| Admin Status | □ |
| Controller | 209.165.200.231 |
| Site Config ID | 0 |

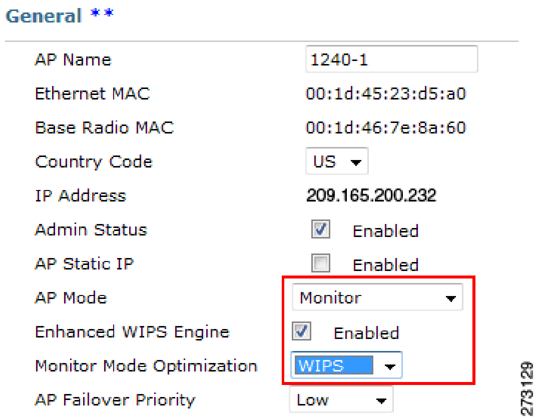
**Step 4** Click **Save**.

> **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 whose radio you just disabled.

**Step 6** In the access point dialog box, choose **Monitor Mode** from the AP Mode drop-down list. (see Figure 6-4).

*Figure 6-4 Configure > Access Points > AP Name*



General **

| | |
|---|---|
| AP Name | 1240-1 |
| Ethernet MAC | 00:1d:45:23:d5:a0 |
| Base Radio MAC | 00:1d:46:7e:8a:60 |
| Country Code | US |
| IP Address | 209.165.200.232 |
| Admin Status | ☑ Enabled |
| AP Static IP | □ Enabled |
| AP Mode | Monitor |
| Enhanced WIPS Engine | ☑ Enabled |
| Monitor Mode Optimization | WIPS |
| AP Failover Priority | 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**.

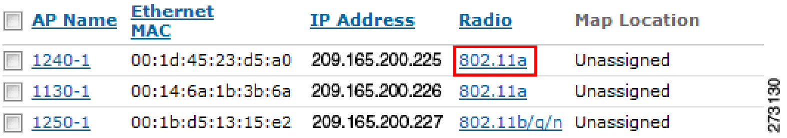
**Step 9** Click **Save**.

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

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

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

*Figure 6-5 Configure > Access Points > Radio*



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

**Step 13** In the radio configuration pane, select the Admin Status **Enabled** check box.

**Step 14** Click **Save**.

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

# Configuring wIPS Profiles

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

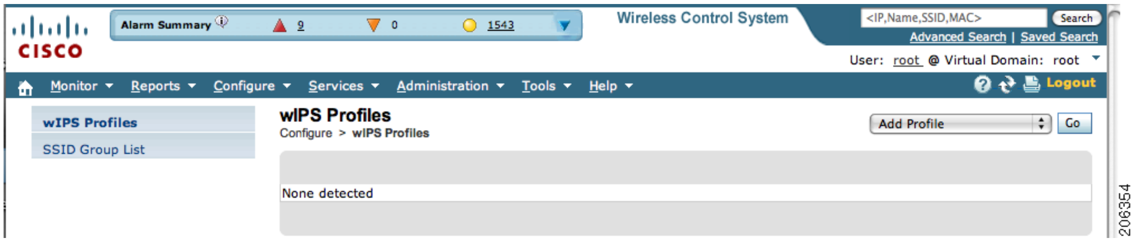
**Note** Some of the configuration steps that follow are marked as *Overlay-Only* and are only to be undertaken when deploying the Adaptive wIPS solution to monitor an existing WLAN Infrastructure such as an autonomous or completely separate controller-based WLAN.

To configure wIPS profiles, follow these steps:

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

**Step 2** In the wIPS Profile page that appears (Figure 6-6), choose **wIPS Profiles**.

*Figure 6-6 WIPS Profiles > Profile List*



wIPS Profiles
Configure > wIPS Profiles

None detected

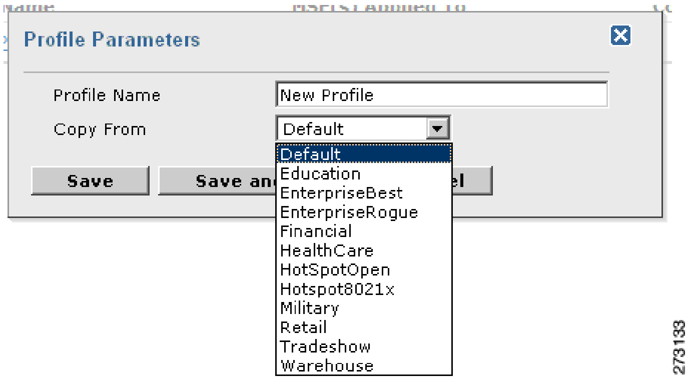
**Step 3** From the Select a command drop-down list, choose **Add Profile** and click **Go**.

**Step 4** In the Profile Parameters dialog box, choose a profile template from the Copy From drop-down list (see Figure 6-7).

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

**Note** You cannot edit the default profile.

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



Profile Parameters

Profile Name: New Profile

Copy From: Default

***Figure 6-7 Profile Parameters Dialog Box***

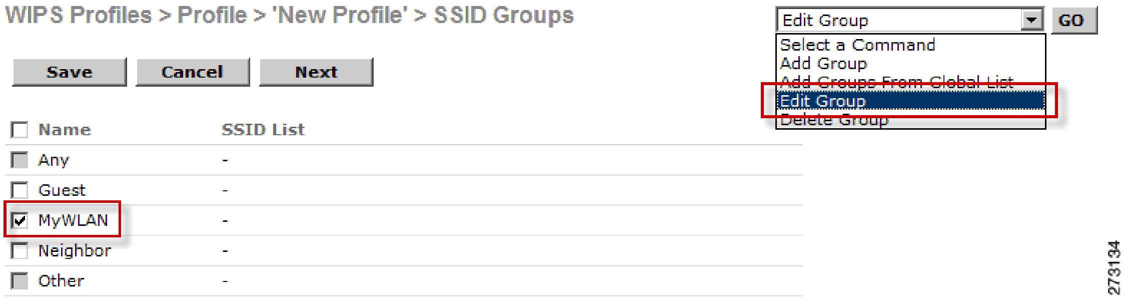
**Step 5** After selecting a profile and entering a profile name, click **Save and Edit**.

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

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

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

***Figure 6-8 SSID Groups Summary Pane***



WIPS Profiles > Profile > 'New Profile' > SSID Groups

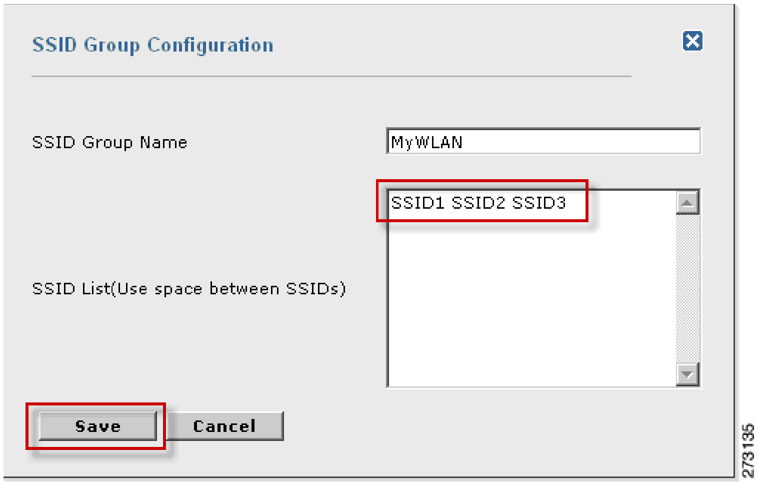
| | Name | SSID List |
|---|---|---|
| □ | Any | - |
| □ | Guest | - |
| ☑ | MyWLAN | - |
| □ | Neighbor | - |
| □ | Other | - |

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** (see Figure 6-9).

*Figure 6-9 SSID Group Configuration Dialog Box*

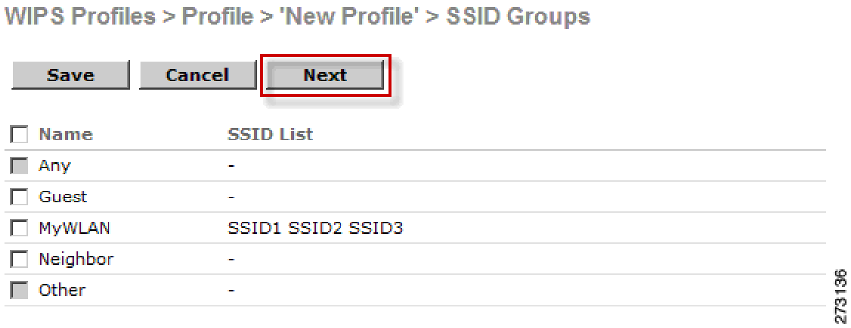


SSID Group Configuration

| | |
|---|---|
| SSID Group Name | MyWLAN |
| SSID List(Use space between SSIDs) | SSID1 SSID2 SSID3 |

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

*Figure 6-10 New Profile > SSID Groups Page*



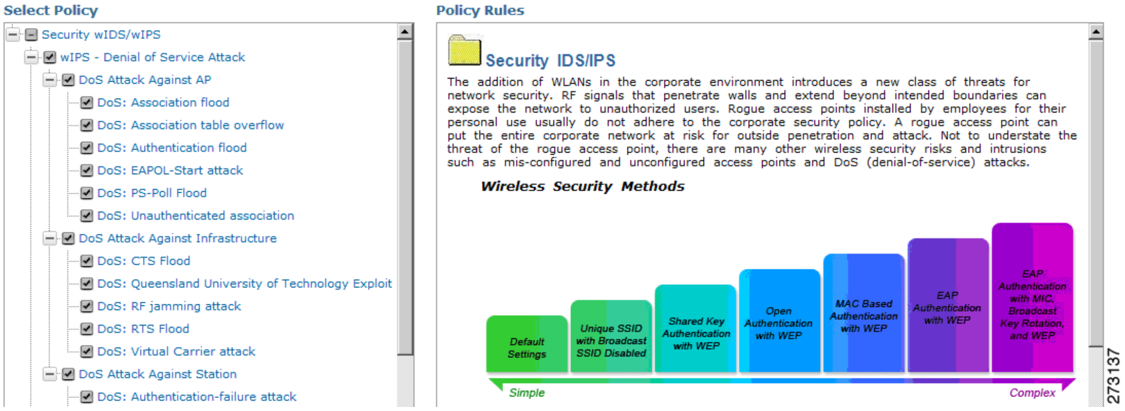
WIPS Profiles > Profile > 'New Profile' > SSID Groups

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

d. Click **Next**.

The Select Policy and Policy Rules summary panes appear (see Figure 6-11).

*Figure 6-11 Next > Select Policy Summary Pane*



Select Policy

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

Policy Rules

Security IDS/IPS

The addition of WLANs in the corporate environment introduces a new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured and unconfigured access points and DoS (denial-of-service) attacks.

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

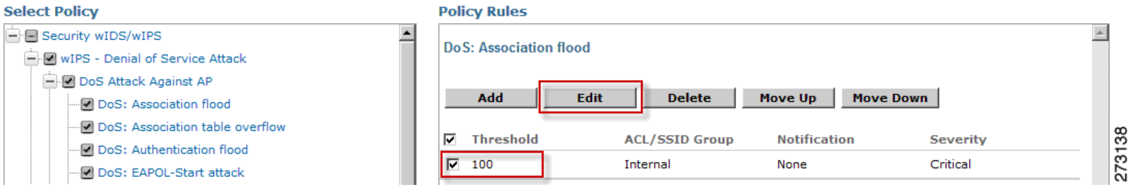
**Note** At the policy page (Figure 6-11), you can enable or disable attacks to be detected and reported. You can also edit specific thresholds for alarms and turn on forensics.

**Step 7** To enable or disable attacks to be detected and reported, select the check box next to the specific attack type in question in the Select Policy pane.

**Step 8** 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 (see Figure 6-12).

***Figure 6-12 Policy Rules Pane***



Select Policy

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

Policy Rules

DoS: Association flood

Add | Edit | Delete | Move Up | Move Down

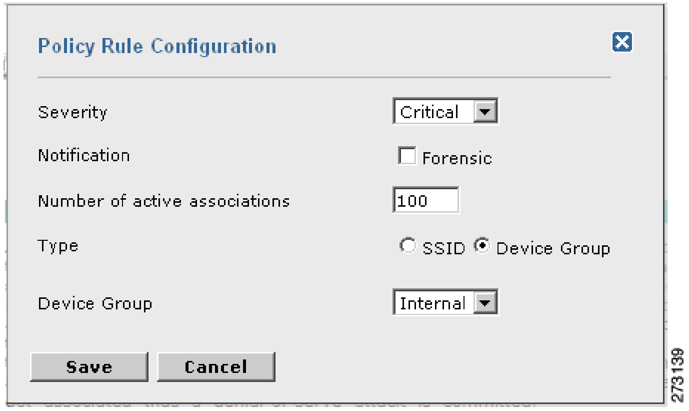
| ☑ Threshold | ACL/SSID Group | Notification | Severity |
|---|---|---|---|
| ☑ 100 | Internal | None | Critical |

**Step 9** 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 6-13).

***Figure 6-13 Policy Rule Configuration Dialog Box***



Policy Rule Configuration ☒

Severity: Critical

Notification: ☐ Forensic

Number of active associations: 100

Type: ○ SSID ● Device Group

Device Group: Internal

Save | Cancel

**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 will monitor for attacks.

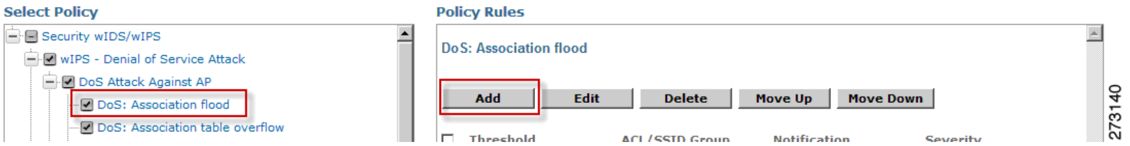
1. If you select SSID, continue with Step 10.
2. If you select Device Group, continue with Step 11.

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

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

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

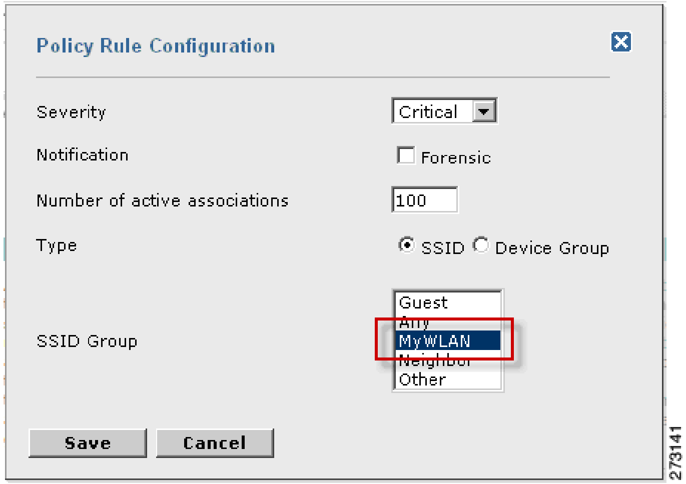
***Figure 6-14 Adding a Policy Rule***



**b.** In the Policy Rule Configuration dialog box, select **MyWLAN** from the SSID Group list (see Figure 6-15).

**Note** SSID is already selected as the type.

***Figure 6-15 Policy Rule Configuration Dialog Box for SSIDs***



Policy Rule Configuration

Severity: Critical

Notification: □ Forensic

Number of active associations: 100

Type: ● SSID ○ Device Group

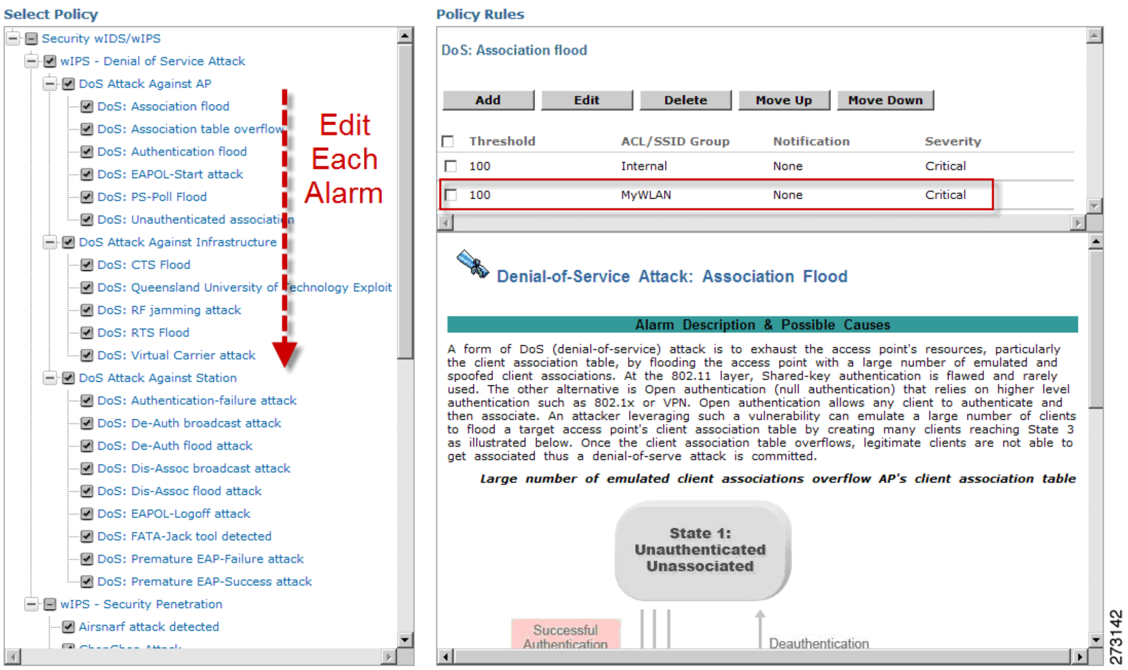
SSID Group: Guest, Any, MyWLAN (selected), Neighbor, Other

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

**d.** Modify each policy rule. Continue with Step 11 when all modifications are complete. (See Figure 6-16).

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

*Figure 6-16 Edit Policy Rules for SSID Monitoring*



Select Policy

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

Policy Rules

DoS: Association flood

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

Denial-of-Service Attack: Association Flood

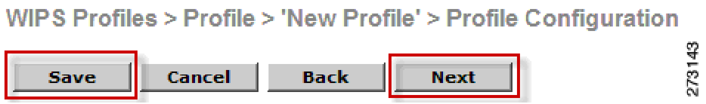
Alarm Description & Possible Causes

A form of DoS (denial-of-service) attack is to exhaust the access point's resources, particularly the client association table, by flooding the access point with a large number of emulated and spoofed client associations. At the 802.11 layer, Shared-key authentication is flawed and rarely used. The other alternative is Open authentication (null authentication) that relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker leveraging such a vulnerability can emulate a large number of clients to flood a target access point's client association table by creating many clients reaching State 3 as illustrated below. Once the client association table overflows, legitimate clients are not able to get associated thus a denial-of-serve attack is committed.

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

**Step 11** In the Profile Configuration dialog box, click **Save** to save the Profile (SSID or Device Group). Click **Next** (see Figure 6-17).

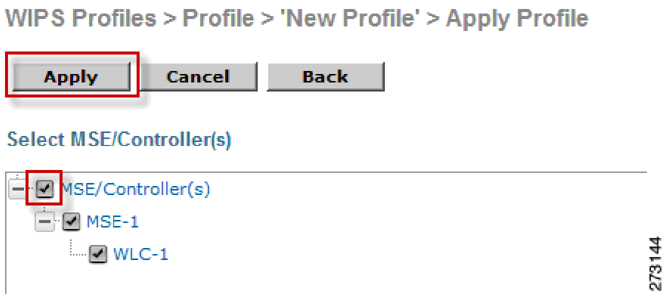
*Figure 6-17 Profile Configuration Dialog box*



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

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

*Figure 6-18 Apply Profile Dialog Box*



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

Select MSE/Controller(s)

- ⊟ ☑ MSE/Controller(s)
  - ⊟ ☑ MSE-1
    - ☑ WLC-1

CHAPTER 7

# Monitoring the System and Services

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

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

This chapter contains the following sections:

- Working with Alarms, page 7-2
- Working with Events, page 7-8
- Working with Logs, page 7-8
- Generating Reports, page 7-10
- Security Reports and Alarms for wIPS, page 7-14

# Working with Alarms

This section describes how to view, assign, and clear alarms and events on a mobility services engine using WCS. It also describes how to have e-mail notifications for alarms sent to you as well as how to define those types (all, critical, major, minor, warning) of alarm notifications.

This section contains the following topics:

- Viewing Alarms, page 7-2
- Viewing MSE Alarm Details, page 7-3
- Assigning and Unassigning Alarms, page 7-5
- Deleting and Clearing Alarms, page 7-6
- Emailing Alarm Notifications, page 7-6

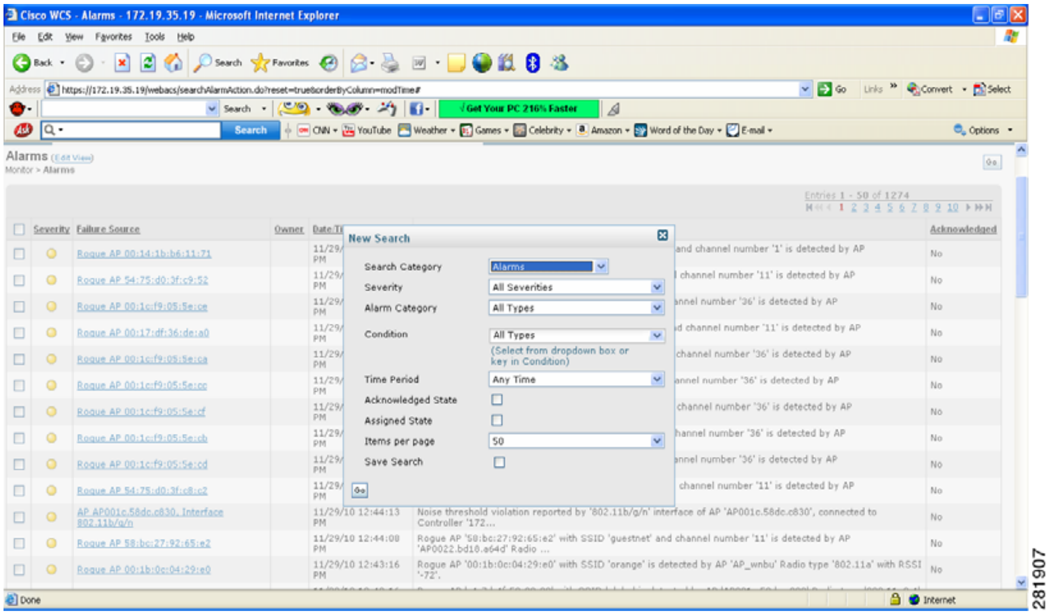
# Viewing Alarms

To view the mobility services engine alarms, follow these steps:

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

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

***Figure 7-1 New Search Alarm Dialog Box***



New Search

Search Category: Alarms
Severity: All Severities
Alarm Category: All Types
Condition: All Types
(Select from dropdown box or key in Condition)
Time Period: Any Time
Acknowledged State: □
Assigned State: □
Items per page: 50
Save Search: □
Go

| □ | Severity | Failure Source | Owner | Date/Ti | | Acknowledged |
|---|---|---|---|---|---|---|
| □ | ● | Rogue AP 00:14:1b:b6:11:71 | | 11/29/ PM | and channel number '1' is detected by AP | No |
| □ | ● | Rogue AP 54:75:d0:3f:c9:52 | | 11/29/ PM | l channel number '11' is detected by AP | No |
| □ | ● | Rogue AP 00:1c:f9:05:5e:ce | | 11/29/ PM | annel number '36' is detected by AP | No |
| □ | ● | Rogue AP 00:17:df:36:de:a0 | | 11/29/ PM | d channel number '11' is detected by AP | No |
| □ | ● | Rogue AP 00:1c:f9:05:5e:ca | | 11/29/ PM | channel number '36' is detected by AP | No |
| □ | ● | Rogue AP 00:1c:f9:05:5e:cc | | 11/29/ PM | annel number '36' is detected by AP | No |
| □ | ● | Rogue AP 00:1c:f9:05:5e:cf | | 11/29/ PM | channel number '36' is detected by AP | No |
| □ | ● | Rogue AP 00:1c:f9:05:5e:cb | | 11/29/ PM | hannel number '36' is detected by AP | No |
| □ | ● | Rogue AP 00:1c:f9:05:5e:cd | | 11/29/ PM | annel number '36' is detected by AP | No |
| □ | ● | Rogue AP 54:75:d0:3f:c8:c2 | | 11/29/ PM | channel number '11' is detected by AP | No |
| □ | ● | AP AP001c.58dc.c830, Interface 802.11b/g/n | | 11/29/10 12:44:13 PM | Noise threshold violation reported by '802.11b/g/n' interface of AP 'AP001c.58dc.c830', connected to Controller '172... | No |
| □ | ● | Rogue AP 58:bc:27:92:65:e2 | | 11/29/10 12:44:08 PM | Rogue AP '58:bc:27:92:65:e2' with SSID 'guestnet' and channel number '11' is detected by AP 'AP0022.bd18.a64d' Radio ... | No |
| □ | ● | Rogue AP 00:1b:0c:04:29:e0 | | 11/29/10 12:43:16 PM | Rogue AP '00:1b:0c:04:29:e0' with SSID 'orange' is detected by AP 'AP_wnbu' Radio type '802.11a' with RSSI '-72'. | No |

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

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

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

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

**Step 6** Choose the time frame for which you want to review alarms from the Time Period drop-down list.

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 7** Select the **Acknowledged State** check box to exclude the acknowledged alarms and their count in the Alarm Summary page.

**Step 8** Select the **Assigned State** check box to exclude the assigned alarms and their count in the Alarm Summary page.

**Step 9** Choose the number of alarms to display on each window from the Items per page drop-down list.

**Step 10** 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 11** Click **Go**. The Alarms summary dialog box appears with the search results.

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

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

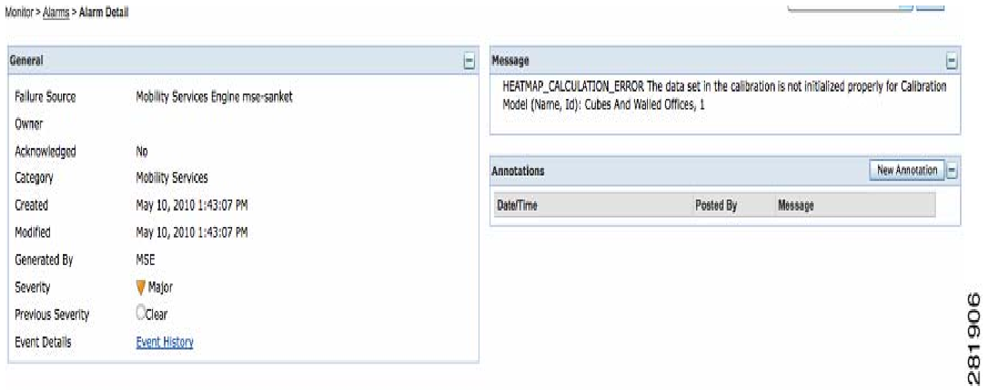
# Viewing MSE Alarm Details

In the **Monitor** > **Alarms** page, click an MSE item under Failure Source to access the alarms details for a particular MSE.

Alternatively, you can access the **Services** > **Mobility Services** > ***MSE Name*** > **System** > **Status** > **WCS Alarms** page and click a particular MSE item under Failure Source to access the alarms details for a particular MSE.

Figure 7-2 shows a WCS Alarm for MSE.

*Figure 7-2 MSE Alarm*



Monitor > Alarms > Alarm Detail

**General**

| | |
|---|---|
| Failure Source | Mobility Services Engine mse-sanket |
| Owner | |
| Acknowledged | No |
| Category | Mobility Services |
| Created | May 10, 2010 1:43:07 PM |
| Modified | May 10, 2010 1:43:07 PM |
| Generated By | MSE |
| Severity | Major |
| Previous Severity | Clear |
| Event Details | Event History |

**Message**

HEATMAP_CALCULATION_ERROR The data set in the calibration is not initialized properly for Calibration Model (Name, Id): Cubes And Walled Offices, 1

**Annotations**

| Date/Time | Posted By | Message |
|---|---|---|

Table 7-1 describes the various fields in the Alarm Detail page for an MSE.

*Table 7-1 General Parameters*

| Parameter | Description |
|---|---|
| Failure Source | The MSE that generated the alarm. |
| Owner | Name of person to which this alarm is assigned, or blank. |
| Acknowledged | Displays whether or not the alarm is acknowledged by the user. |
| Category | The category of the alarm. The Alarm category is Mobility Services for MSEs. |
| Created | Month, day, year, hour, minute, second, AM or PM alarm created. |
| Modified | Month, day, year, hour, minute, second, AM or PM alarm last modified. |
| Generated By | This field will display 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 box and click **Add** to update the alarm. Notes appear in the “Annotations” display area.
- Messages—Displays information about the alarm.
- Audit Report—Click to view config audit alarm details. This report is only available for config audit alarms.

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

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

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

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

### Select a Command

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

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

**Note** Once the severity is Clear, the alarm is deleted from WCS after 30 days.

- Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in WCS 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 email notifications.
- Event History—Takes you to the Monitor > Events page to view events for this alarm.

## Assigning and Unassigning Alarms

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

**Step 1** Choose **Monitors** > **Alarms** to display the Alarms page as described in the "Viewing Alarms" section on page 7-2.

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

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

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

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

## Deleting and Clearing Alarms

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

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

**Step 1** Choose **Monitors** > **Alarms** to display the Alarms page as described in the "Viewing Alarms" section on page 7-2.

**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**.

## Emailing Alarm Notifications

WCS lets you send alarm notifications to a specific e-mail address. Sending notifications through e-mail enables you to take prompt action when needed.

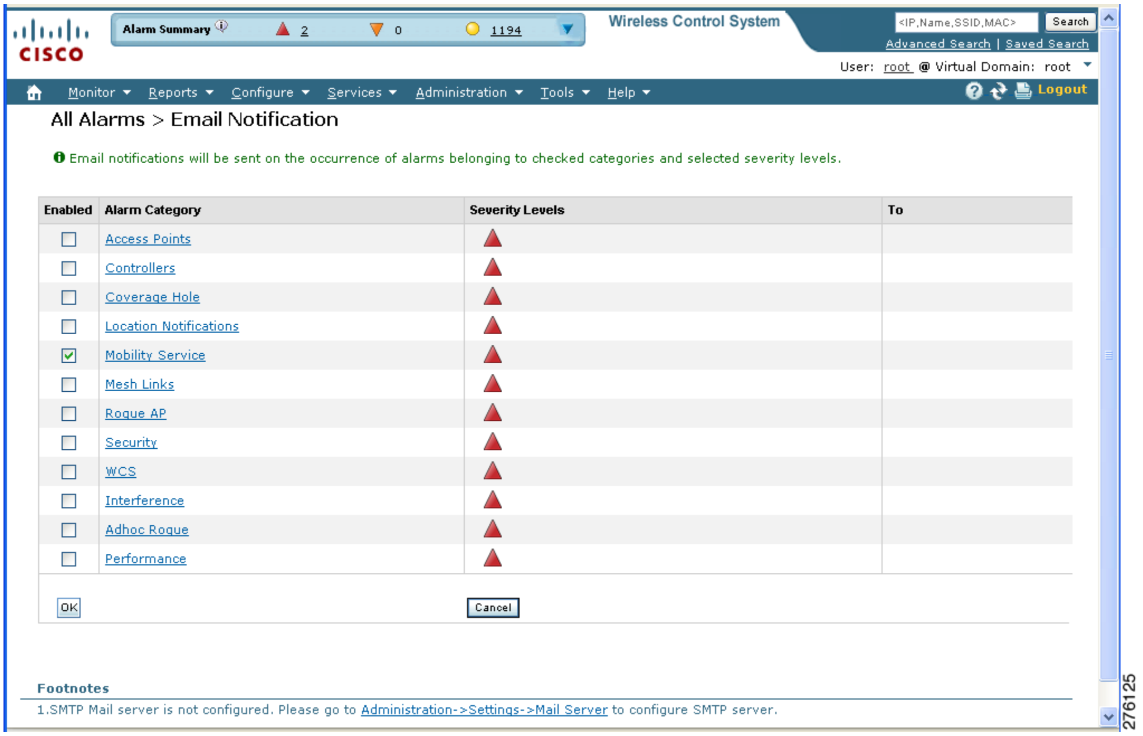
You can select the alarm severity types (critical, major, minor, and warning) you have emailed to you.

To send alarm notifications, follow these steps:

**Step 1** Choose **Monitor > Alarms**.

**Step 2** From the Select a commands drop-down list, choose **Email Notification**. Click **Go**. The Email Notification page appears (see Figure 7-3).

*Figure 7-3 All Alarms > Email Notification page*



All Alarms > Email Notification

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

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

OK Cancel

Footnotes

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

**Note** An SMTP Mail Server must be defined prior to entry of 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 the 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**.

The Alarms > Notification page appears. 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 WCS to view mobility services engine and location notification events. You can search and display events based on their severity (critical, major, minor, warning, clear, info) and event category.

You can search by the following event categories:

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

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

- By security

Additionally, you can search for events of an element by its IP address, MAC address or name.

A successful event search displays the event severity, failure object, date and time of the event, and any messages for each event.

To display events, follow these steps:

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

**Step 2** In the Events page:

- 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. Click **Search**.
- To display events by severity and category, click **Advanced Search** in the navigation bar and choose the appropriate options from the Severity and Event Category drop-down lists. Click **Go**.

**Step 3** If WCS finds events that match the search criteria, it displays a list of these events.

**Note** For more information about an event, click the failure object associated with the event. Additionally, you can sort the events summary by each of the column headings.

# Working with Logs

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

This section contains the following topics:

- Configuring Logging Options, page 7-9
- Downloading Log Files, page 7-10

# Configuring Logging Options

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

To configure logging options, follow these steps:

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

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

**Step 3** From the System left sidebar menu click **Logs**. The advanced parameters for the selected mobility services engine appears.

**Step 4** In the Logging Options section, choose the appropriate option from the Logging Level drop-down list.

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

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

**Step 5** Select the **Enabled** 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.

**Step 7** To download log files from the server, click **Download Logs**. For more information, see Downloading Log Files.

**Step 8** In the Log File Parameters section, 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 Parameters section, 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.

**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 backup or rollover log file.

The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC Address. The MAC log files 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 WCS to download them to your system. WCS downloads a zip file containing the log files.

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

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

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

**Step 3** Choose **System > Logs**.

**Step 4** Click **Download Logs**.

**Step 5** Follow the instructions in the File Download dialog box to open the file or save the zip file to your system.

# Generating Reports

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

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

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

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

You can view the following in a location utilization report:

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

This section contains the following topics:

- Creating a Device Utilization Report, page 7-10
- Viewing Saved Utilization Reports, page 7-13
- Viewing Scheduled Utilization Runs, page 7-13

## Creating a Device Utilization Report

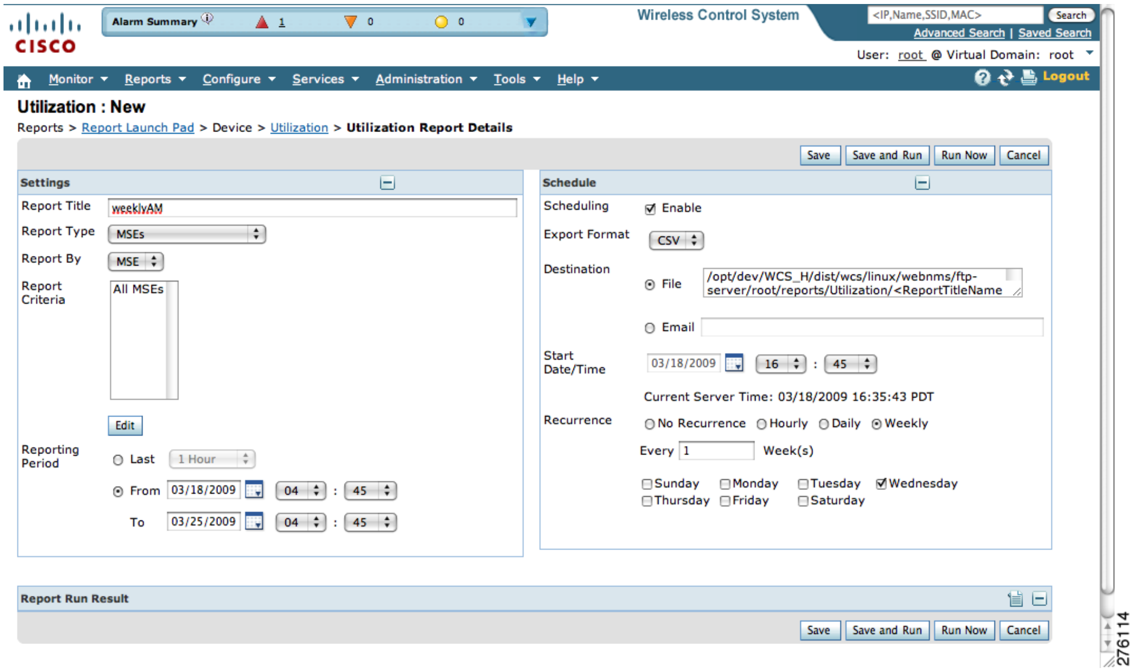
To create a utilization report for the mobility services engine, follow these steps:

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

**Step 2** Choose **Device > Utilization**.

**Step 3** Click **New**. The Utilization: New page appears (see Figure 7-4).

*Figure 7-4 Device > Utilization New Page*



User: root @ Virtual Domain: root

Utilization : New

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

**Settings**

Report Title: weeklyAM

Report Type: MSEs

Report By: MSE

Report Criteria: All MSEs

Reporting Period: ○ Last 1 Hour

● From 03/18/2009 04 : 45

To 03/25/2009 04 : 45

**Schedule**

Scheduling: ☑ Enable

Export Format: CSV

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

○ Email

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

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

Recurrence: ○ No Recurrence ○ Hourly ○ Daily ● Weekly

Every 1 Week(s)

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

**Report Run Result**

**Step 4** In the Settings pane, enter a report title.

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

**Step 6** Click **Edit** to select either a specific mobility services engine or **All MSEs** in the dialog box that appears.

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

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

**Step 8** In the Schedule pane, select the **Enable Schedule** check box.

**Step 9** Choose the report format (CSV or PDF) from the Export Report drop-down list.

**Step 10** Select either the **File** or **Email** radio button 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 11** Enter a start date (MM:DD:YYYY) or click the calendar icon to select a date.

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

**Step 13** Select any one of the Recurrence options to determine how often the report is to be run.

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

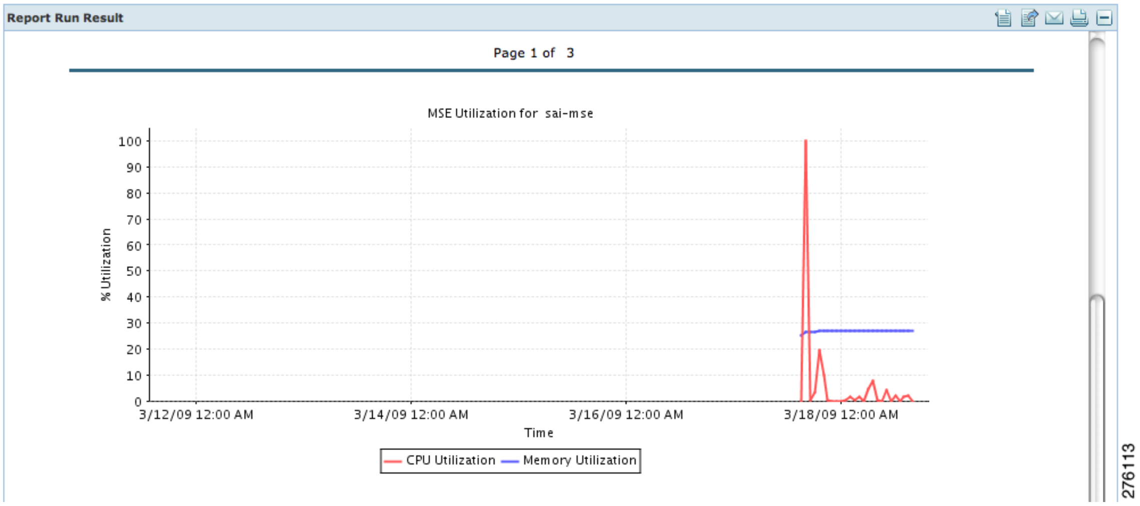
**Step 14** When finished with all of the above steps, do one of the following:

- Click **Save** to save edits. The report is run at the designated time and the results are either 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 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 pane.
- Click **Run Now** if you want to run the report immediately and review the results in the WCS 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.
- Click **Export Now** to export the results to a CSV or PDF format.
- In the results page, click **Cancel** to cancel the defined report.

The results appear at the bottom of the page (see Figure 7-4).

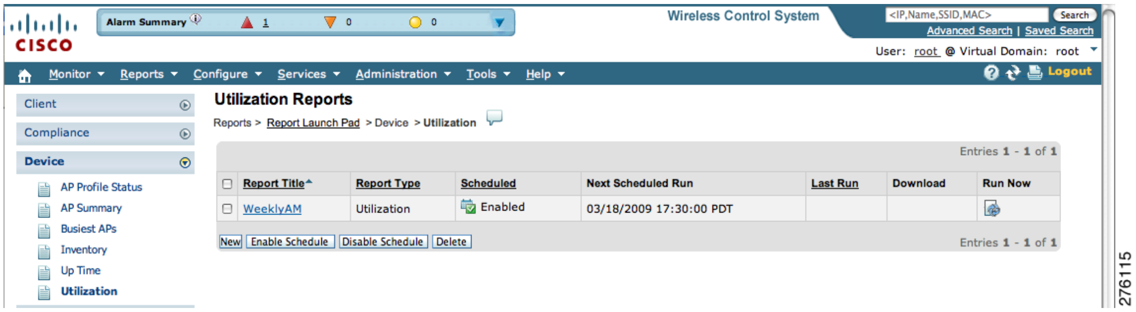
**Note** Only the CPU and memory utilization reports are shown (see Figure 7-5).

*Figure 7-5 Device > MSE Utilization > Results*



**Step 15** If you clicked Save or Save and Run, 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 (see Figure 7-6).

***Figure 7-6 Utilization Reports Page***



Utilization Reports

Reports > Report Launch Pad > Device > Utilization

Entries 1 - 1 of 1

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

Entries 1 - 1 of 1

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

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

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

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

## Viewing Saved Utilization Reports

To download a saved report, follow these steps:

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

**Step 2** Click the **Download** icon for your request. 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** In WCS, choose **Reports > Scheduled Runs**.

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

**Step 3** Click the **Download** icon for your report. It is downloaded and saved in the defined directory or 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—Displays all adhoc events that WCS has received in the selected timeframe.
- Adhoc Rogues—Displays all adhocs that have been updated in the selected timeframe.
- New Rogue APs—Displays, in tabular form, all rogues detected in a selected timeframe. It provides which new rogues were detected within a selected time. The created time indicates the time at which the rogue was first detected.
- New Rogue AP Count—Displays, in graphical form, all rogues detected in a selected timeframe.
- Rogue APs—Displays all rogues that are active in your network and have been updated in the selected timeframe. WCS receives updated events for rogues that are detected.
- Rogue APs Event—Displays all the events received by WCS. The controller sends updates of detected rogues if any of the attributes change or new rogues are detected.

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

- Security Summary—Shows the number of association failures, rogues access points, ad hocs, and access point connections or disconnections over one month.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any scheduled time associated with the report and is viewable 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 7-15
- Viewing Saved wIPS Report, page 7-17
- Viewing Scheduled wIPS Report Runs, page 7-17

# 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:

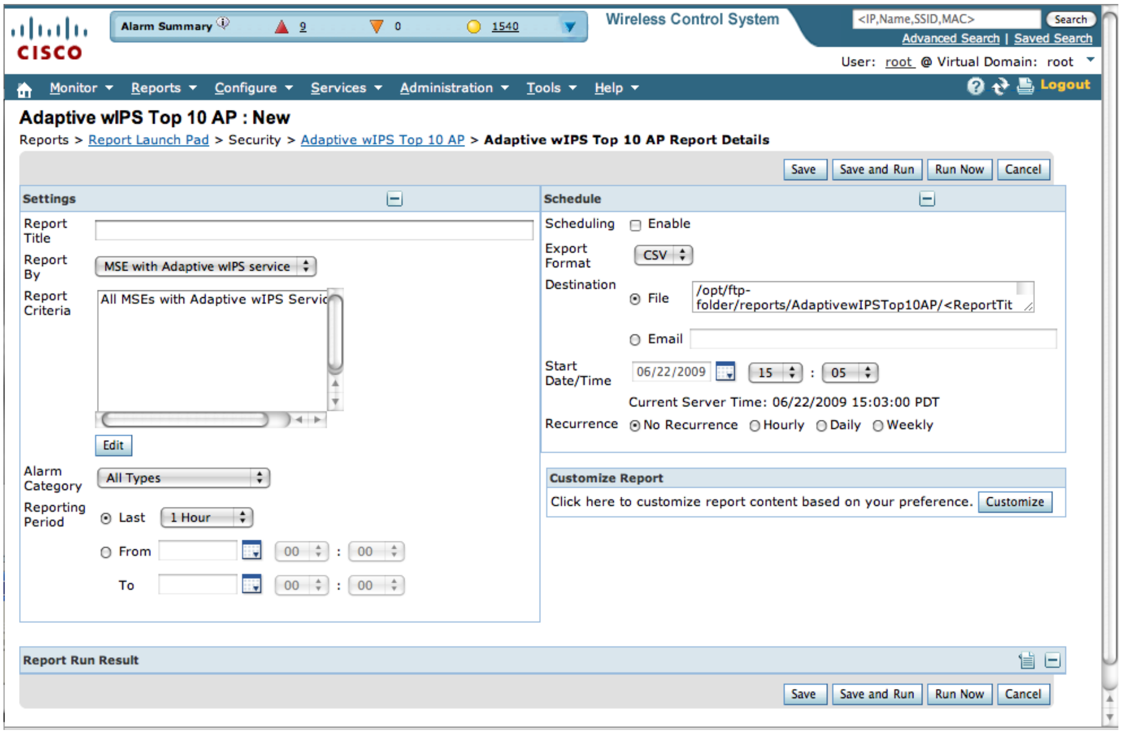
**Note** Some of these steps or options are not required for every report.

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

**Step 2** Choose **Security** and click on 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 (see Figure 7-7).

***Figure 7-7 New Report Page***



User: root @ Virtual Domain: root

Adaptive wIPS Top 10 AP : New

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

Settings

Report Title:

Report By: MSE with Adaptive wIPS service

Report Criteria: All MSEs with Adaptive wIPS Servic

Alarm Category: All Types

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

Schedule

Scheduling: □ Enable

Export Format: CSV

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

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

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

Recurrence: ● No Recurrence ○ Hourly ○ Daily ○ Weekly

Customize Report

Click here to customize report content based on your preference.

Report Run Result

**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 will display on the x-axis.

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

**Step 9** In the Schedule panel, 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 at 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 only appear on the when the weekly option is chosen.

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 panel.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any pending, scheduled run of that report. Results appear the bottom of the 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 panel.
  - 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 WCS 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 Saved wIPS Report

To download a saved report, follow these steps:

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

**Step 2** 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** In WCS, choose **Reports > Scheduled Runs**.

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

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

CHAPTER 8

# Performing Maintenance Operations

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

This chapter contains the following sections:

- Recovering a Lost Password, page 8-1
- Recovering a Lost Root Password, page 8-2
- Backing Up and Restoring Mobility Services Engine Data, page 8-2
- Downloading Software to Mobility Services Engines, page 8-4
- Configuring the NTP Server, page 8-6
- Resetting the System, page 8-6

## Recovering a Lost Password

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

**Step 1** When the GRUB (GRand Unified Bootloader) screen comes up, press **Esc** to enter the boot menu.

**Step 2** Press **e** to edit.

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

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

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

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.

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

# Recovering a Lost Root Password

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

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

**Step 2** Press **e** to edit.

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

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

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

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

**Note** The shell prompt does not appear if you 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:

- Backing Up Mobility Services Engine Historical Data, page 8-2
- Restoring Mobility Services Engine Historical Data, page 8-3
- Enabling Automatic Data Backup, page 8-4

## Backing Up Mobility Services Engine Historical Data

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

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

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

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

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

**Step 3** Choose **System > Maintenance > Backup**.

**Step 4** Enter the name of the backup.

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

**Step 6** Click **Submit** to back up the historical data to the hard drive of the server running WCS.

The status of the backup can be seen on the screen while the backup is in process. Three items will appear on the screen during the backup process: (1)The Last Status text box provides messages noting the status of the backup; (2) The Progress text box shows what percentage of the backup is complete; and (3) The Started at text box 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 other WCS pages.

**Note** Backups are stored in the FTP directory you specify during the WCS installation.

# Restoring Mobility Services Engine Historical Data

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

**Note** You cannot run the restore process in the background while working on other mobility services engine operations in other WCS pages.

To restore mobility services engine data, follow these steps:

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

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

**Step 3** Choose **System > Maintenance > Restore**.

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

**Step 5** Select the **Delete synchronized service assignments** check box if you want to permanently removes 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 do any future location calculations.

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

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

## Enabling Automatic Data Backup

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

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

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

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

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

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

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

**Step 6** Click **Submit**.

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

# Downloading Software to Mobility Services Engines

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

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

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

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

**Step 4** Choose **System > Maintenance > Download Software**.

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

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

  The WCS downloads the binary images listed in the drop-down list into the FTP server directory you specified during the WCS installation.

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

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

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

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

**Step 9** Run the installer image from the /opt/installers directory by entering:

```
./.bin mse image.
```

This installs the software.

**Step 10** To run the software, enter:

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

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

## Manually Downloading Software

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

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

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

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

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

Your entries should look like this example:

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

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

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

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

The decompression yields a bin file.

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

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

**Step 4** Enter the following command:

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

to install the new mobility services engine image.

**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, refer to the *Cisco 3350 Mobility Services Engine Getting Started Guide* or *Cisco 3310 Mobility Services Engine Getting Started Guide* at the following link: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html
- If you need to add or change an NTP server installation after a mobility services engine install, rerun the automatic installation script. You can configure the NTP server without adjusting the other values by just tabbing through the script.

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

# Resetting the System

For information on rebooting or shutting down the mobility services engine hardware, see the Rebooting or Shutting Down a System, page 4-11.

# Clearing the Configuration File

For information on clearing the configuration file, see the Clearing the System Database, page 4-12.

APPENDIX A

# wIPS Policy Alarm Encyclopedia

This appendix provides an overview of the threat types addressed by wIPS and consists of 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 understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured and unconfigured access points and DoS (Denial of Service) attacks.

The Cisco Adaptive Wireless IPS (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.

### Pre-configured 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:

- Enterprise best practice

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

When the administrator selects the appropriate profile, the wIPS will enable or disable 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 will be enabled. The administrator still has the option after installation to enable or disable any alarm or change the threshold values as per individual preferences.

The wIPS system not only is an IDS (Intrusion Detection System), but also is 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-21

# 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 a 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. Cisco has developed Management Frame Protection, the basis of 802.11i, to proactively prevent many of these attacks. (For more information on MFP, refer to the Cisco WCS online help.) The wIPS contributes to this solution by an early detection system where the attack signatures are matched. The DoS of the wIPS detection focuses on WLAN layer one (physical layer) and two (data link layer, 802.11, 802.1x). When strong WLAN authentication and encryption mechanisms are used, higher layer (IP layer and above) DoS attacks are difficult to execute. The wIPS server tightens your WLAN defense by validating strong authentication and encryption policies. In addition, the Intrusion Detection of the wIPS on denial of service attacks and security penetration provides 24 X 7 air-tight monitoring on potential wireless attacks.

Denial of service attacks include the following three subcategories:

- Denial of Service Attack Against Access Points, page A-3
- Denial of Service Attack Against Infrastructure, page A-8

- Denial of Service Attacks Against Client Station, page A-12

# Denial of Service Attack Against Access Points

DoS attacks against access points are typically carried out on the basis of the following assumptions:

- Access points have limited resources. For example, the per-client association state table.
- WLAN management frames and authentication protocols 802.11 and 802.1x have no encryption mechanisms.

Wireless intruders can exhaust access point resources, most importantly the client association table, by emulating large number of wireless clients with spoofed MAC addresses. Each one of these emulated clients attempts association and authentication with the target access point but leaves the protocol transaction mid-way. When the access point's 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, refer to the WCS online help.

DoS attacks against access points include: the following types:

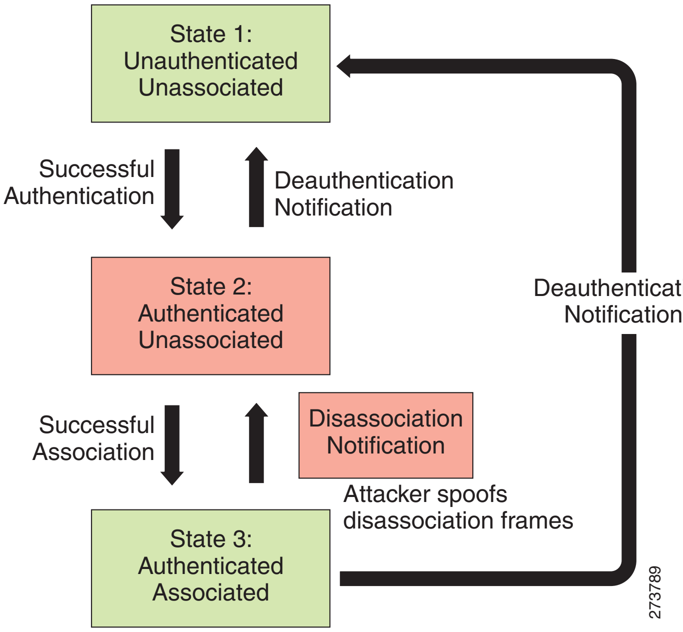
  - Denial of Service Attack: Association Flood, page A-3
  - Denial of Service Attack: Association Table Overflow, page A-4
  - Denial of Service Attack: Authentication Flood, page A-5
  - Denial of Service Attack: EAPOL-Start Attack, page A-6
  - Denial of Service Attack: PS Poll Flood Attack, page A-6
  - 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 A-1).

*Figure A-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, refer to the *Cisco Wireless Control System Configuration Guide* or the WCS 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.

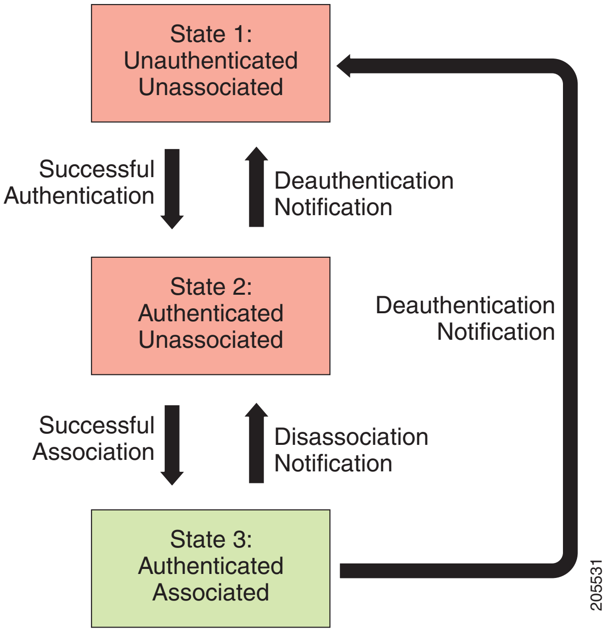
## Denial of Service Attack: Authentication Flood

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 A-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 A-2 Authentication Flood*


State 1: Unauthenticated Unassociated
Successful Authentication
Deauthentication Notification
State 2: Authenticated Unassociated
Deauthentication Notification
Successful Association
Disassociation Notification
State 3: Authenticated Associated
205531

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

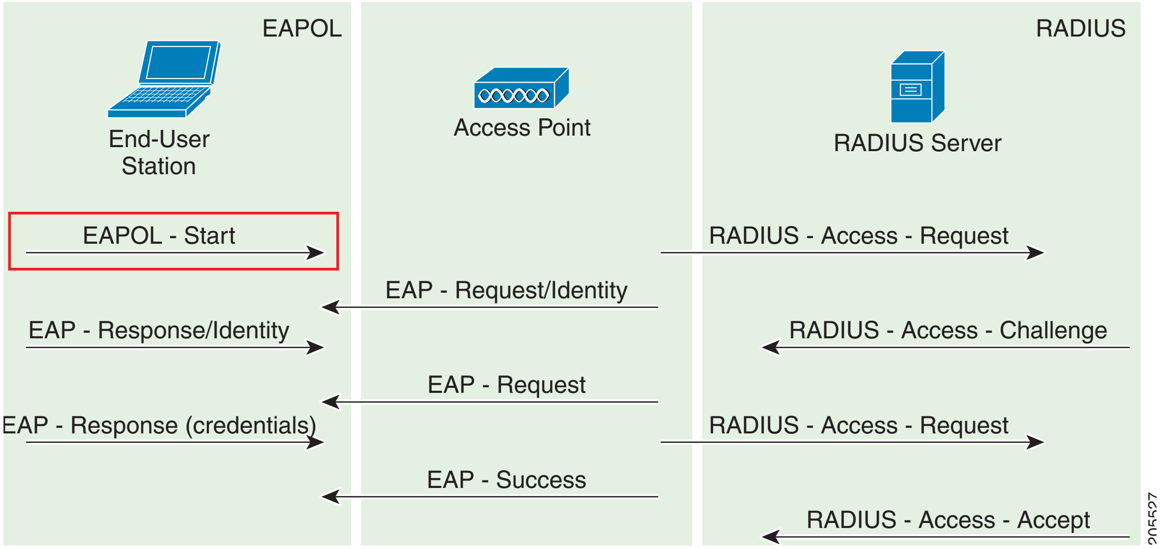
The wIPS detects this form of DoS attack by tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security analyst can log onto the access point to check the current association table status.

## 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 A-3).

*Figure A-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 will be in the sleep mode (power save mode). At the end of the time period, the client wakes up and checks for waiting data frames. After it completes a handshake with the access point, it receives the data frames. The beacons from the access point also include the Delivery Traffic Indication Map (DTIM) to inform the client when it needs to wake up to accept multicast traffic.

The access point continues to buffer data frames for the sleeping wireless clients. Using the Traffic Indication Map (TIM), the access point notifies the wireless client that it has buffered data buffered. Multicast frames are sent after the beacon that announces the DTIM.

The client requests the delivery of the buffered frames using PS-Poll frames to the access point. For every PS-Poll frame, the access point responds with a data frame. If there are more frames buffered for the wireless client, the access point sets the data bit in the frame response. The client then sends another PS-Poll frame to get the next data frame. This process continues until all the buffered data frames are received.

A potential hacker could spoof the MAC address of the wireless client and send out a flood of PS-Poll frames. The access point then sends out the buffered data frames to the wireless client. In reality, the client could be in the power safe mode and would miss the data frames.

### wIPS Solution

The 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, refer to the *Cisco Wireless Control System Configuration Guide* or the WCS 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, refer to the *Cisco Wireless Control System Configuration Guide* or the WCS online help.

# 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: CTS Flood, page A-8
- Denial of Service Attack: Queensland University of Technology Exploit, page A-9
- Denial of Service attack: RF Jamming Attack, page A-10
- Denial of Service: RTS Flood, page A-11
- Denial of Service Attack: Virtual Carrier Attack, page A-11

## Denial of Service Attack: CTS Flood

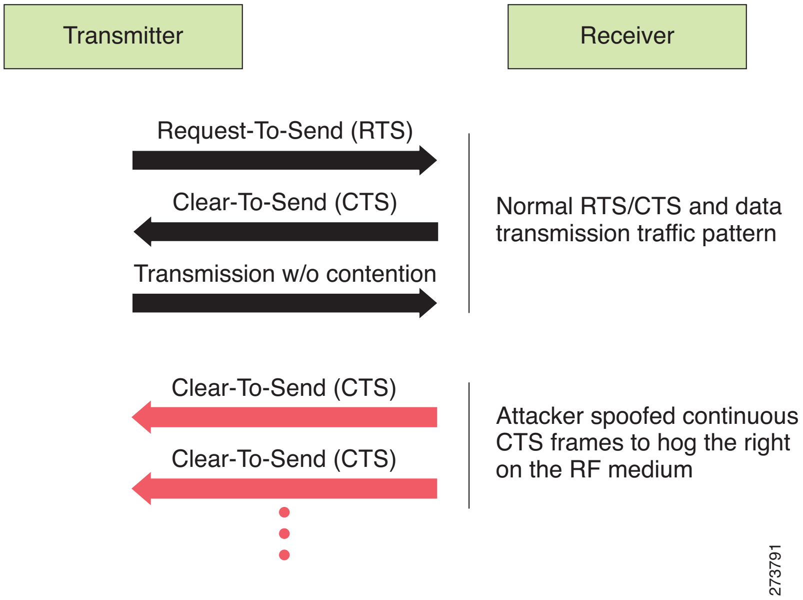
Attack tool: CTS Jack

### 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 A-4).

*Figure A-4 CTS Spoof and Challenge to RF Control*


Transmitter
Receiver
Request-To-Send (RTS)
Clear-To-Send (CTS)
Transmission w/o contention
Normal RTS/CTS and data transmission traffic pattern
Clear-To-Send (CTS)
Clear-To-Send (CTS)
Attacker spoofed continuous CTS frames to hog the right on the RF medium
273791

### 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 could potentially make it vulnerable to DoS radio frequency jamming attacks.

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

This DoS attack affects DSSS WLAN devices including IEEE 802.11, 802.11b, and low-speed (below 20Mbps) 802.11g wireless devices. IEEE 802.11a (using OFDM), high-speed (above 20Mbps using OFDM) 802.11g wireless devices are not affected by this attack. Devices that use FHSS are also not affected.

Any attacker using a PDA or a laptop equipped with a WLAN card can launch this attack on SOHO and enterprise WLANs. Switching to the 802.11a protocol is the only solution or known protection against this DoS attack.

For more information on this DoS attack, refer to:

- www.isrc.qut.edu.au
- http://www.auscert.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, refer to the *Cisco Wireless Control System Configuration Guide* or the WCS online help.

## Denial of Service: RTS Flood

### Alarm Description and Possible Causes

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

A wireless denial of service attacker may take advantage of the privilege granted to the CTS frame to reserve the RF medium for transmission. By transmitting back-to-back RTS frames with a large transmission duration text box, an attacker reserves the wireless medium and force other wireless devices sharing the RF medium to hold back their transmissions.

### wIPS Solution

The 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 my be part of a MAC level fragmented packet) and when observing a CTS.

A station that receives an RTS frame also receives the data frame. The IEEE 802.11 standard specifies the exact times for the subsequent CTS and data frames. The duration value of RTS is respected until the following data frame is received or not received. Either the observed CTS is unsolicited or the observing node is a hidden terminal. If this CTS is addressed to a valid in-range station, the valid station can nullify this by sending a zero duration null function frame. If this CTS is addressed to an out-of-range station, one method of defense is to introduce authenticated CTS frames containing cryptographically signed copies of the preceding RTS. With this method, there is a possibility of overhead and feasibility issues.

### wIPS Solution

The wIPS detects this DoS attack. Locate the device and take appropriate steps to remove it from the wireless environment.

# Denial of Service Attacks Against Client Station

DoS attacks against wireless client stations are typically carried out based upon 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:

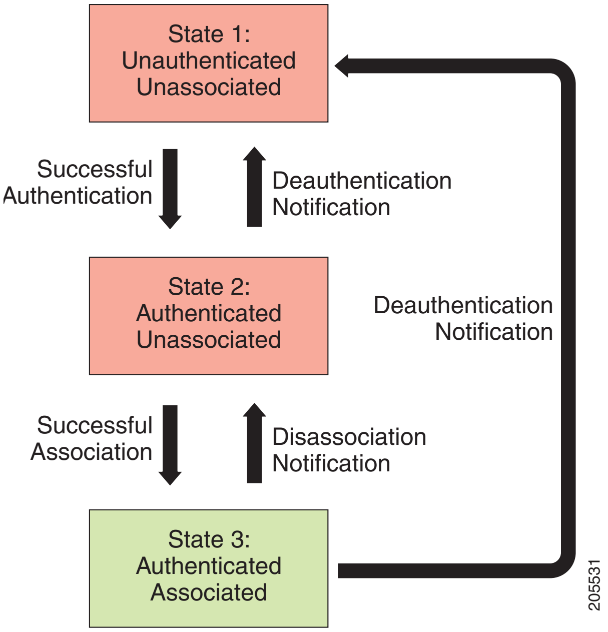
- "Denial of Service Attack: Authentication Failure Attack" section on page A-12
- "Denial of Service Attack: Deauthentication Broadcast" section on page A-13
- "Denial of Service Attack: Disassociation Flood" section on page A-16
- "Denial of Service Attack: EAPOL Logoff Attack" section on page A-18
- "Denial of Service Attack: FATA Jack Tool Detected" section on page A-18
- "Denial of Service Attack: Premature EAP Failure Attack" section on page A-20
- "Denial of Service Attack: Premature EAP Success Attack" section on page A-21

## 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 A-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 A-5 Authentication Failure Attack*


State 1: Unauthenticated Unassociated
Successful Authentication
Deauthentication Notification
State 2: Authenticated Unassociated
Deauthentication Notification
Successful Association
Disassociation Notification
State 3: Authenticated Associated
205531

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.

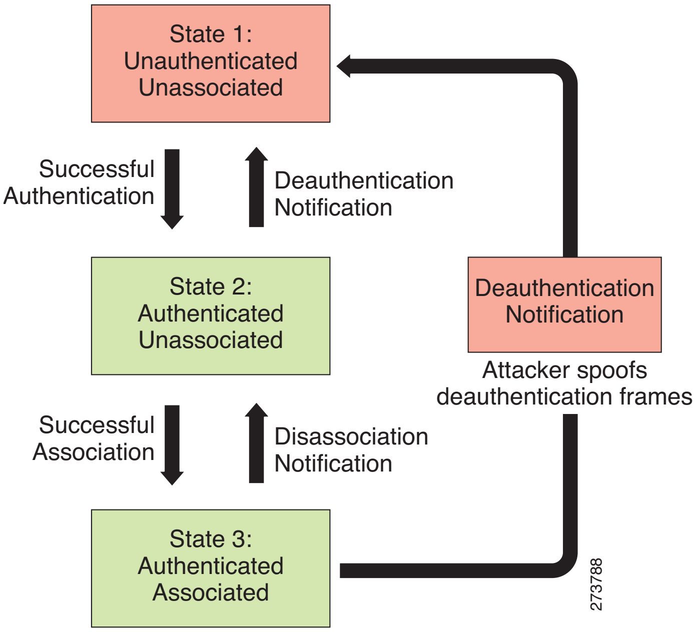
## Denial of Service Attack: Deauthentication Broadcast

Attack tool: WLAN Jack, Void11, Hunter Killer

### Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client 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 A-6).

***Figure A-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 wIPS detects this form of DoS attack by detecting spoofed deauthentication frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security analyst can log onto the access point to verify the current association table status.

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

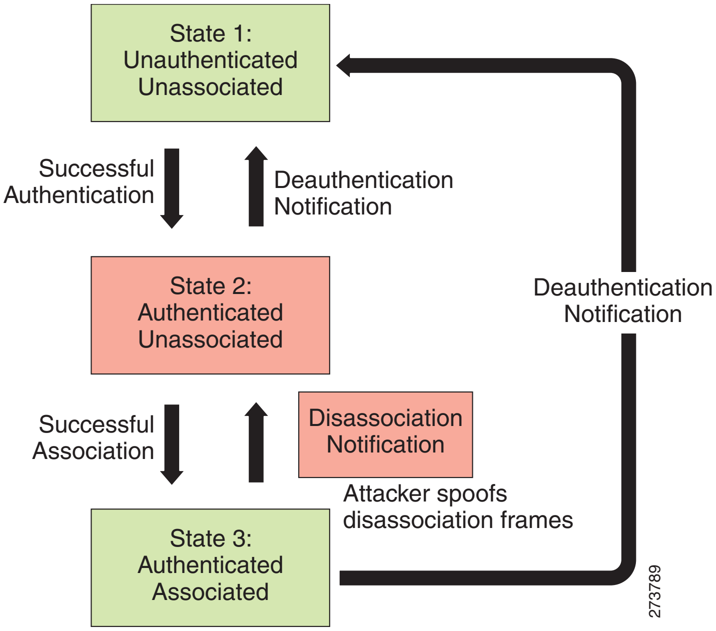
## Denial of Service Attack: Deauthentication Flood

Attack tool: WLAN Jack, Void11

### Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client 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 A-7).

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

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

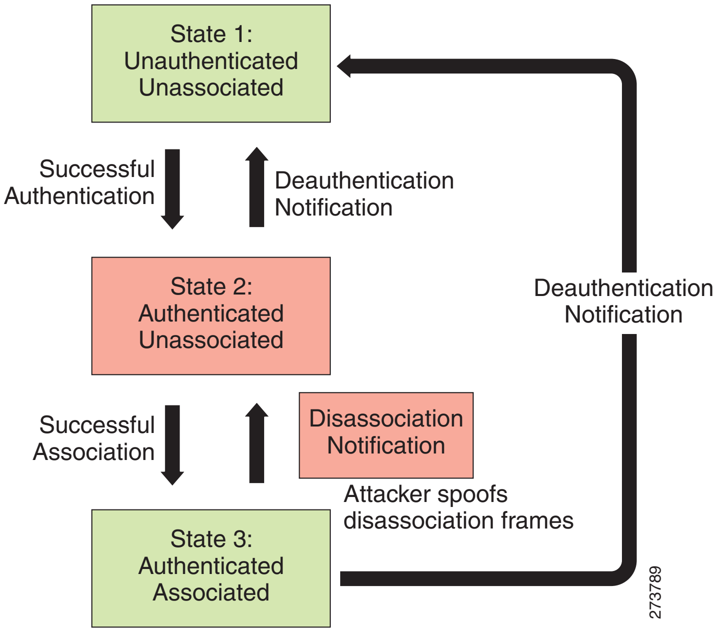
## Denial of Service Attack: Disassociation Broadcast

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 can not participate in WLAN data communication until it is authenticated and associated to State 3 (see Figure A-8).

***Figure A-8 Disassociation Broadcast Attack***


State 1: Unauthenticated Unassociated
Successful Authentication
Deauthentication Notification
State 2: Authenticated Unassociated
Deauthentication Notification
Successful Association
Disassociation Notification
Attacker spoofs disassociation frames
State 3: Authenticated Associated
273789

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, refer to the *Cisco Wireless Control System Configuration Guide* or the WCS online help.

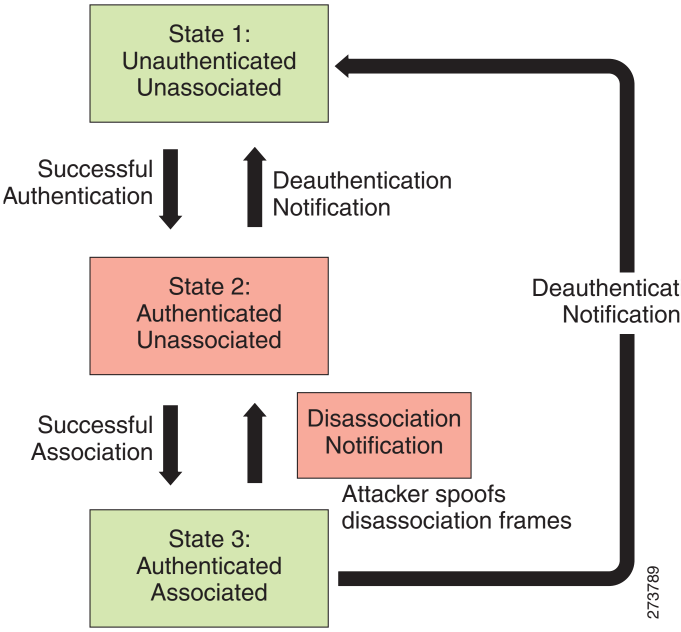
## Denial of Service Attack: Disassociation Flood

Attack tool: ESSID Jack

## Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client stays in State 3 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 A-9).

*Figure A-9 Disassociation Flood Attack*


State 1: Unauthenticated Unassociated
Successful Authentication
Deauthentication Notification
State 2: Authenticated Unassociated
Deauthentication Notification
Successful Association
Disassociation Notification
Attacker spoofs disassociation frames
State 3: Authenticated Associated
273789

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

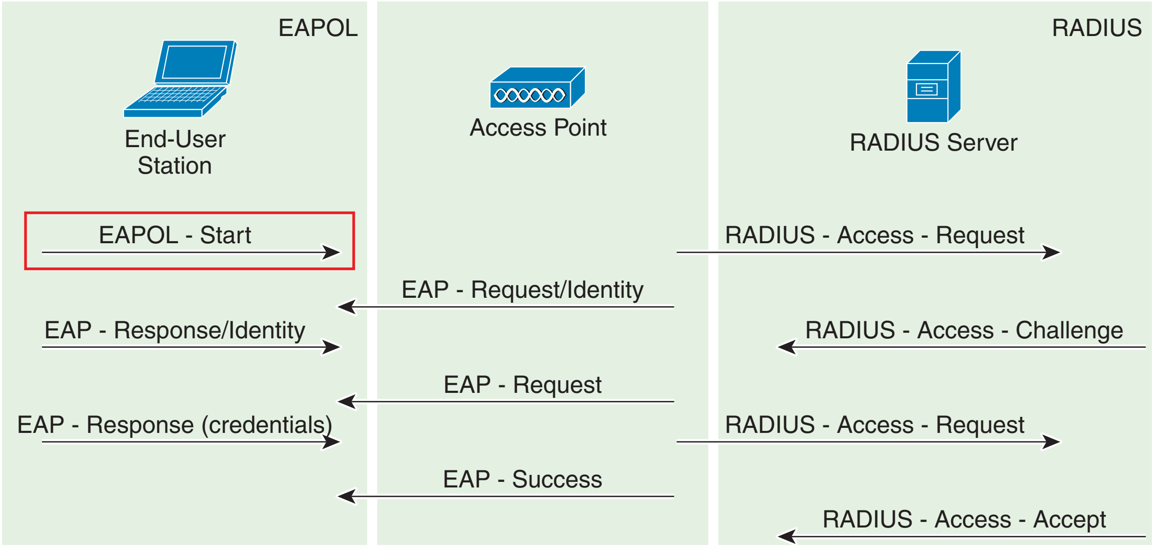
The wIPS detects this form of DoS attack by detecting spoofed disassociation frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log onto the access point to check the current association 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 A-10).

*Figure A-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 re-associates and authenticates automatically to regain the wireless connection. The attacker can continuously transmit the spoofed EAPOL-logoff frames to be effective on this attack.

### wIPS Solution

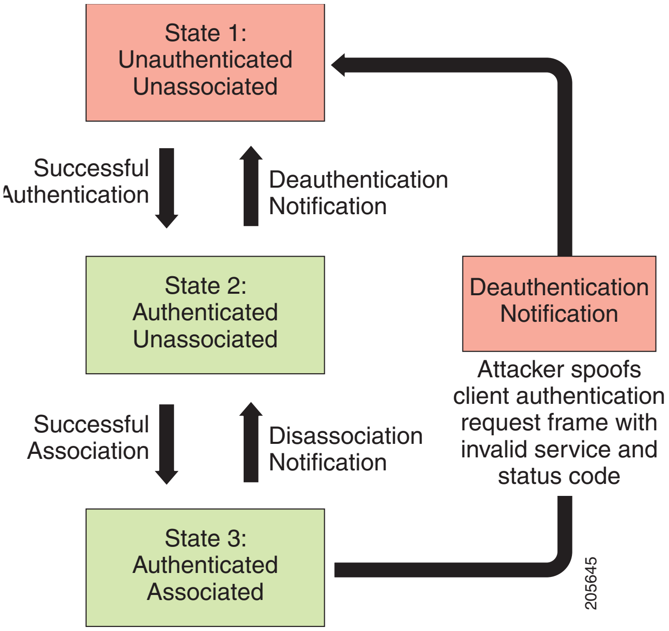
The wIPS detects this form of DoS attack by tracking 802.1x authentication states. When the alarm is triggered, the client and access point under attack are identified. The WLAN security officer logs onto the access point to check the current association table status.

## 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 A-11).

*Figure A-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.

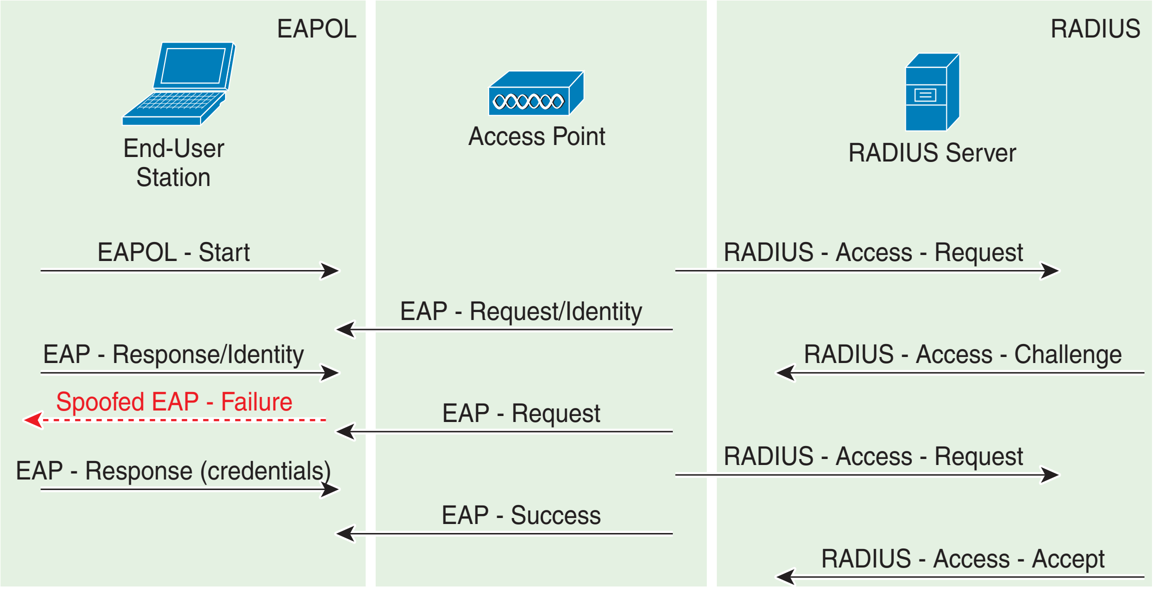
Cisco Management Frame Protection also provides complete proactive protection against frame and device spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide* or the WCS online help.

# Denial of Service Attack: Premature EAP Failure Attack

## 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 A-12).

*Figure A-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 pre-mature EAP-failure frames from the access point to the client to disrupt the authentication state on the client.

## wIPS Solution

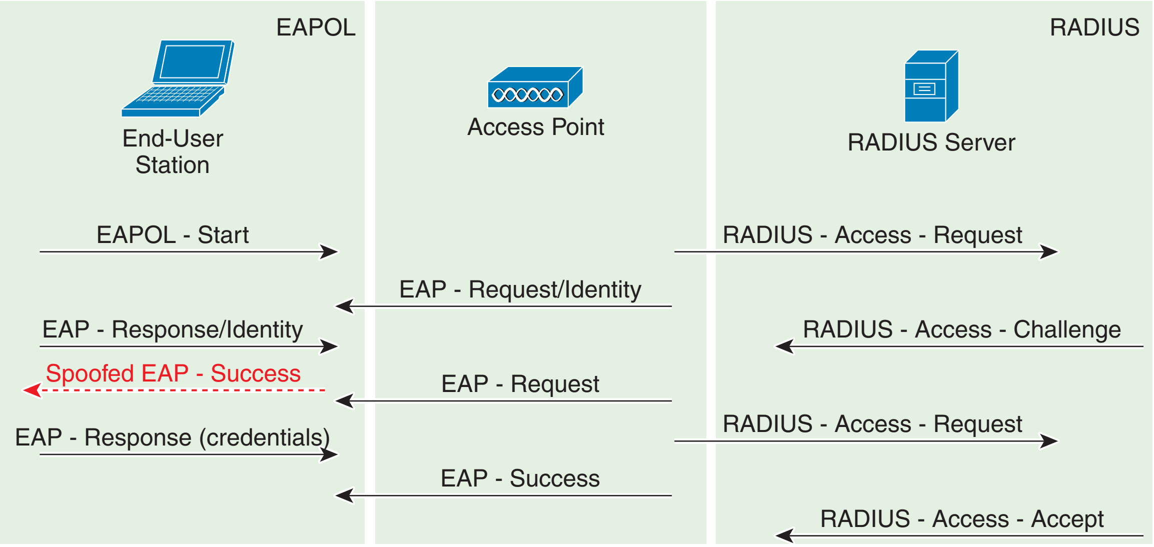
The wIPS detects this form of DoS attack by tracking the spoofed premature EAP-failure frames and the 802.1x authentication states for each client station and access point. Find the device and remove it from the wireless environment.

## Denial of Service Attack: Premature EAP Success Attack

### 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 A-13).

*Figure A-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.

# Intrusion Detection—Security Penetration

A form of wireless intrusion is to breach the WLAN authentication mechanism to gain access to the wired network or the wireless devices. Dictionary attacks on the authentication method is a common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked access point attack on a unsuspicious wireless client may fool the client into associating with faked access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.

These security threats can be prevented if mutual authentication and strong encryption techniques are used. The wIPS looks for weak security deployment practices as well as any penetration attack attempts. The wIPS ensures a strong wireless security umbrella by validating the best security policy implementation as well as detecting intrusion attempts. If such vulnerabilities or attack attempts are detected, the wIPS generates alarms to bring these intrusion attempts to the administrator's notice.

Security penetration attacks include the following types:

- Airsnarf Attack Detected, page A-23
- Potential Chopchop Attack in Progress, page A-24
- Day-0 Attack by WLAN Performance Anomaly, page A-24
- Day-0 Attack by WLAN Security Anomaly, page A-26
- Day-0 Attack by Device Performance Anomaly, page A-27
- Day-0 Attack by Device Security Anomaly, page A-29
- Device Probing for Access Points, page A-30
- Dictionary Attack on EAP Methods, page A-32
- EAP Attack Against 802.1x Authentication, page A-32
- Fake Access Points Detected, page A-33
- Fake DHCP Server Detected (Potential Wireless Phishing), page A-33
- Fast WEP Crack (ARP Replay) Detected, page A-34
- Potential Fragmentation Attack in Progress, page A-35
- Hot-Spotter Tool Detected (Potential Wireless Phishing), page A-35
- Malformed 802.11 Packets Detected, page A-36
- Man-in-the-Middle Attack Detected, page A-37
- Monitored Device Detected, page A-38
- NetStumbler Detected, page A-38
- NetStumbler Victim Detected, page A-39
- Publicly Secure Packet Forwarding (PSPF) Violation, page A-39
- Potential ASLEAP Attack Detected, page A-40
- Potential Honeypot AP Detected, page A-42
- Soft AP or Host AP Detected, page A-42
- Spoofed MAC Address Detected, page A-42
- Suspicious After-Hours Traffic Detected, page A-43
- Unauthorized Association by Vendor List, page A-43
- Unauthorized Association Detected, page A-44
- Wellenreiter Detected, page A-44

## Airsnarf Attack Detected

### 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 login 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 login credentials for the subscribers. Most hotspot controllers verify subscribers' credentials with the authentication server.

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

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

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

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

### wIPS Solution

The wIPS detects the wireless device running the Airsnarf tool. Appropriate action must be taken by the administrator to remove the Airsnarf tool from the WLAN environment.

## Potential Chopchop Attack in Progress

### Alarm Description and Possible Causes

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

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 PGRA 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 will try 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.

## Day-0 Attack by WLAN Performance Anomaly

### Alarm Description and Possible Causes

WLAN performance efficiency is constantly challenged by the dynamics of the RF environment and the mobility of client devices. A closely monitored and well tuned WLAN system can achieve a higher throughput than a poorly managed one. Radio Resource Management (RRM) built into the Cisco Unified Wireless Network monitors and dynamically corrects performance issues found in the RF environment. Further performance anomaly monitoring may be done via the Wireless IPS system. For more information on RRM, refer to the WCS 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 re-transmission
  - 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 could 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-0 Attack by WLAN Security Anomaly

### Alarm Description and Possible Causes

The addition of WLANs in the corporate environment introduces a whole new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk of outside penetration and attack. Besides rogue access points, there are many other wireless security vulnerabilities which compromise the wireless network such as misconfigured and unconfigured access points. There can also be DoS (denial of service) attacks from various sources against the corporate network.

WCS provides automated security vulnerability assessment within the wireless infrastructure that proactively reports any security vulnerabilities or mis-configurations. Further assessment may be done over-the-air via the Wireless IPS system. With the comprehensive suite of security monitoring technologies, the 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 unsuspicious wireless client may fool the client into associating with a

fake access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.

- Intrusion detection on denial of service attacks—Wireless DoS (denial of service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLAN at layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example, RF jamming attack with high power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

### wIPS Solution

The 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 check if they are compromising the Enterprise wireless network in any way (attack or vulnerability). If this is an increase in the number of rogue devices, it may indicate an attack against the network. The WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find it.

If there is a sudden increase in the number of client devices with encryption disabled, it may be necessary to revisit the Corporate Security Policy and enforce users to use the highest level of encryption and authentication according to the policy rules.

## Day-0 Attack by Device Performance Anomaly

### Alarm Description and Possible Causes

WLAN performance efficiency is constantly challenged by the dynamics of the RF environment and the mobility of client devices. A closely monitored and well tuned WLAN system can achieve a higher throughput than a poorly managed one. Radio Resource Management built into the Cisco Unified Wireless Network monitors and dynamically corrects performance issues found in the RF environment. Further performance anomaly monitoring may be done via the Wireless IPS system. For more information on RRM, refer to the WCS 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 re-transmission
  - Frame speed (1, 2, 5.5, 11, ... Mbps) usage and distribution
  - Layer 2 frame fragmentation
  - Access point and station association/reassociation/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 could 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 QoS (quality-of-service) features and multimedia support to the existing 802.11 a/b/g wireless standard. This is done while maintaining full backward compatibility with these standards. The QoS feature is critical to voice and video applications. Wireless LAN has limited bandwidth and high overheads as compared to the traditional wired Ethernet. The throughput is reduced for a variety of reasons including the RTS/CTS mechanism, packet fragmentation, packet retransmission, acknowledgements, and collisions.

To maximize the power of the wIPS, performance alarms can be customized to best match your WLAN deployment specification. For example, if your WLAN is designed for all users to use 5.5 and 11 Mb/s speed only, customize the threshold for performance alarm 'Low speed tx rate exceeded' to reflect such an expectation.

## wIPS Solution

The wIPS detects a device violating a large number of performance intrusion policies. This device has either generated a large number of performance intrusion violations in the time period specified or there is a sudden percentage increase as specified in the threshold settings for the various alarms. It is suggested that the device is monitored and located to carry out further analysis to check if this device is causing any issues in the overall performance of the network.

For example, if there is a device which has caused an increase in the number of "access points overloaded by stations" and "access points overloaded by utilization" alarms, this could indicate that the access point cannot handle the stations. The administrator may need to reconsider re-deployment of the access points.

## Day-0 Attack by Device Security Anomaly

### Alarm Description and Possible Causes

The addition of WLANs in the corporate environment introduces a new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. Rogue access points can put the entire corporate network at risk for outside penetration and attack. Besides rogue access points, there are many other wireless security vulnerabilities which compromise the wireless network such as misconfigured and unconfigured access points. There can also be DoS attacks from various sources against the corporate network.

WCS provides automated security vulnerability assessment within the wireless infrastructure that proactively reports any security vulnerabilities or mis-configurations. Further assessment may be done over-the-air via the Wireless IPS system. With the comprehensive suite of security monitoring technologies, the 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 unsuspicious wireless client may fool the client into associating with a fake access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.
- Intrusion detection on DoS attacks—Wireless DoS (denial of service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLAN at layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example, RF jamming attack with high power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

### wIPS Solution

The wIPS detects a device violating a large number of Security IDS/IPS policies. This device has either generated a number of Security IDS/IPS violations in the time period specified or there is a sudden percentage increase as specified in the threshold settings for the various alarms. The device should be monitored and located to carry out further analysis to check if this device is compromising the Enterprise

Wireless Network in any way (attack or vulnerability). If this is a rogue device, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find it.

## Device Probing for Access Points

Some commonly used scan tools include: NetStumbler (newer versions), MiniStumbler (newer versions), MACStumbler, WaveStumbler, PrismStumbler, dStumbler, iStumbler, Aerosol, Boingo Scans, WiNc, AP Hopper, NetChaser, Microsoft Windows XP scans.

### Alarm Description and Possible Causes

The wIPS detects wireless devices probing the WLAN and attempting association (such as association request for an access point with any SSID).

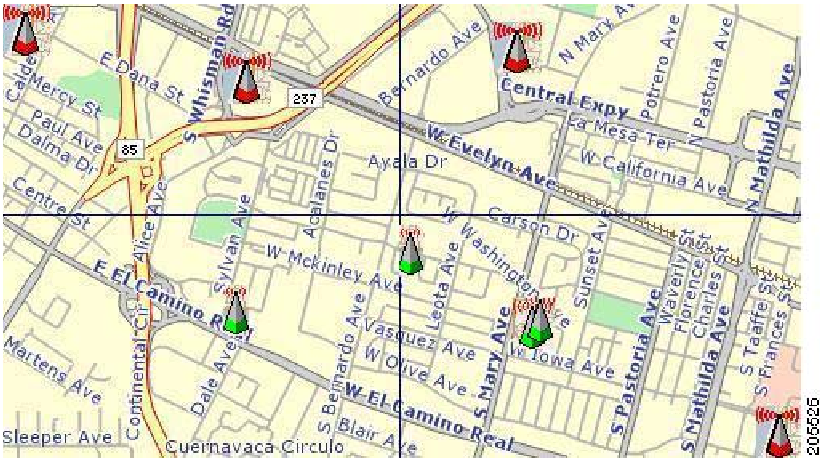
Such devices could pose potential security threats in one of the following ways:

- War-driving, WiLDing (Wireless LAN Discovery), war-chalking, war-walking, war cycling, war-lightrailing, war-busing, and war-flying.
- Legitimate wireless client attempting risky promiscuous association.

War-driving, war-chalking, war-walking, and war-flying activities include:

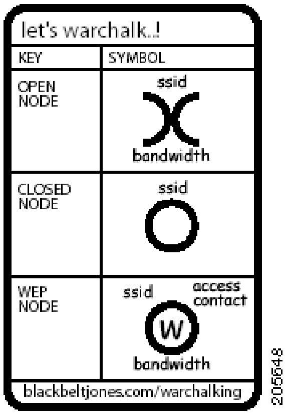
- War-driving—A wireless hacker uses war-driving tools to discover access points and publishes information such as MAC address, SSID, and security implemented on the Internet with the access points' geographical location information (see Figure A-14).

*Figure A-14 Access Point Locations Posted on the Internet*



- War-chalking—War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols (see Figure A-15).

*Figure A-15 War Chalker Universal Symbols*



- War-walking—War-walking is similar to war-driving, but the hacker is on foot instead of a car.
- War-flying—War-flying refers to sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet relay chat sessions from an altitude of 1,500 feet on a war-flying trip.

### Legitimate Wireless Client Attempting Risky Association

The second potential security threat for this alarm may be more damaging. Some of these alarms could be from legitimate and authorized wireless clients on your WLAN who are attempting to associate with any available access point including your neighbor'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 NetStumbler website (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or more recent operating systems. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to search shopping malls and retail stores.

### wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure the access points to not broadcast SSIDs. Use the wIPS to determine which access points are broadcasting (announcing) their SSID in the beacons.

## Dictionary Attack on EAP Methods

### Alarm Description and Possible Causes

EEE 802.1x provides an EAP framework for wired or wireless LAN authentication. An EAP framework allows flexible authentication protocol implementation. Some implementations of 802.1x or WPA use authentication protocols such as LEAP, MD5, OTP (one-time-password), TLS, and TTLS. Some of these authentication protocols are based upon 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 login attempts. A dictionary attack can also take place offline, where an attacker captures a successful authentication challenge protocol exchange and then tries to match the challenge response with all possible password combinations. Unlike online attacks, offline attacks are not easily detected. Using a strong password policy and periodically expiring user passwords significantly reduces an offline attack tool's success.

### wIPS Solution

The 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 upon 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 Access Points Detected

### Alarm Description and Possible Causes

The Fake AP tool is meant to protect your WLAN acting as a decoy to confuse war-drivers using NetStumbler, Wellenreiter, MiniStumbler, Kismet, and so on. The tool generates beacon frames imitating thousands of counterfeit 802.11b access points. War-drivers encountering a large number of access points cannot identify the real access points deployed by the user. This tool, although very effective in fending off war-drivers, poses other disadvantages such as bandwidth consumption, misleading legitimate client stations, and interference with the WLAN management tools. Running the Fake AP tool in your WLAN is not recommended.

### wIPS Solution

The administrator should locate the device running the Fake AP tool and remove it from the wireless environment.

## Fake DHCP Server Detected (Potential Wireless Phishing)

### 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 could be a wireless/wired gateway. Other wireless devices can have the DHCP service running innocently or maliciously so as to disrupt the WLAN IP service. Wireless clients that are requesting an IP address from the DHCP server may then connect to these fake DHCP servers to get their IP address because the clients do not have any means to authenticate the server. These fake DHCP servers may give the clients non-functional network configurations or divert all the client's traffic through them. The hackers can then eavesdrop on every packet sent by the client. With the aid of rogue DNS servers, the hacker could also send the users to fake web page logins to get username and password credentials. It could also give out non-functional and non-routable IP addresses to achieve a DoS attack. This sort of attack is generally against a WLAN without encryption such as hotspots or trade show networks.

### wIPS Solution

The 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 (ARP Replay) Detected

### Alarm Description and Possible Causes

It is well publicized that WLAN devices using static WEP key for encryption are vulnerable to WEP key cracking attack (Refer to *Weaknesses in the Key Scheduling Algorithm of RC4* - I by Scott Fluhrer, Itsik Mantin, and Adi Shamir).

The WEP secret key that has been cracked by any intruder results in no encryption protection, thus leading to compromised data privacy. The WEP key that is in most cases 64-bit or 128-bit (few vendors also offer 152-bit encryption) consists of the secret key specified by the user linked with the 24-bit IV (Initialization Vector). The IV that is determined by the transmitting station can be reused frequently or in consecutive frames, thus increasing the possibility of the secret key to be recovered by wireless intruders.

The most important factor in any attack against the WEP key is the key size. For 64-bit WEP keys, around 150K unique IVs and for 128-bit WEP keys around 500k to a million unique IVs should be enough. With insufficient traffic, hackers have created a unique way of generating sufficient traffic to perform such an attack. This is called the replay attack based on arp-request packets. Such packets have a fixed length and can be spotted easily. By capturing one legitimate arp-request packet and resending them repeatedly, the other host responds with encrypted replies, providing new and possibly weak IVs.

### wIPS Solution

The 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.

WCS also provides automated security vulnerability scanning that proactively reports any access points configured to utilize weak encryption or authentication. For more information on automated security vulnerability scanning, refer to the WCS online help.

## Potential Fragmentation Attack in Progress

### Alarm Description and Possible Causes

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

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.

## Hot-Spotter Tool Detected (Potential Wireless Phishing)

### Alarm Description and Possible Causes

A hotspot is any location where Wi-Fi network access available for the general public. Hotspots are often found in airports, hotels, coffee shops, and other places where business people tend to congregate. It is currently one of the most important network access service for business travelers. The customer requires a wireless-enabled laptop or handheld to connect to the legitimate access point and to receive service. Most hotspots do not require the user to have an advanced authentication mechanism to connect to the access point, other than using a web page to log in. The criterion for entry is only dependent on whether or not the subscriber has paid subscription fees. In a wireless hotspot environment, no one should trust anyone else. Due to current security concerns, some WLAN hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user.

Basic components of a WLAN Hotspot network

The four components of a basic hotspot network are:

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

*Hotspotter* automates a method of penetration against wireless clients, independent of the encryption mechanism used. Using the Hotspotter tool, the intruder can passively 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.

## 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 screen or lock-up problem during the attack period should consider upgrading the WLAN NIC driver or the firmware.

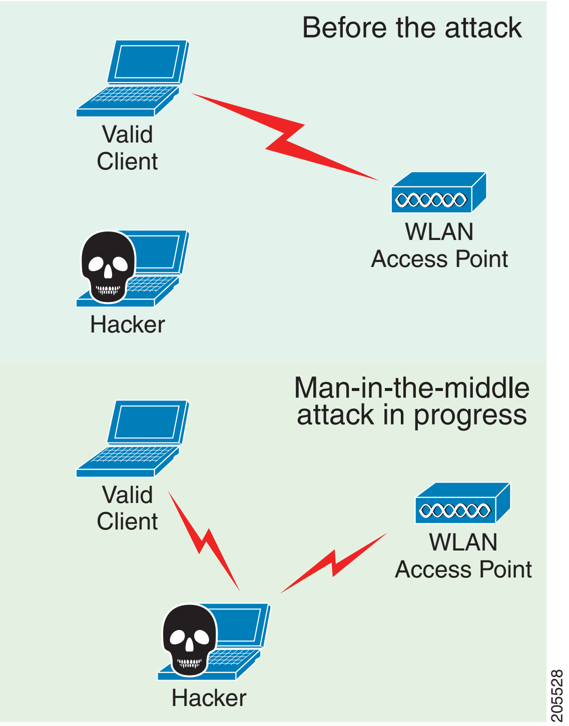
When the client is identified and reported by the wIPS, the WLAN administrator may use the device locator to locate it.

## 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 A-16).

***Figure A-16 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, refer to the *Cisco Wireless Control System Configuration Guide* or the WCS online help.

## Monitored Device Detected

### Alarm Description and Possible Causes

There are some cases in which the access points and STAs activity must be continuously monitored:

- Malicious intruders attempting to hack into the enterprise wired network must be monitored. It is important to keep track of these access points and STAs to help avoid repeated rogue-related and intrusion attempt problems.
- Lost enterprise wireless equipment must be located.
- Vulnerable devices with previous security violations must be monitored.
- Devices used by ex-employees who may have not returned all their wireless equipment must be monitored.

These nodes may be added to the monitor list to alert the wireless administrator the next time the access point or STA shows up in the RF environment.

### wIPS Solution

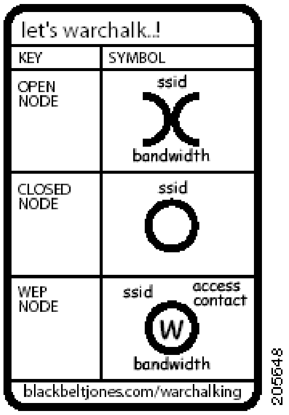
The wireless administrator can add the access point or STA to the monitor list by identifying it as a monitored device on the wIPS.

## 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 A-17).

*Figure A-17 War-Chalker Universal Symbols*



NetStumbler is the most widely used tool for war-driving and war-chalking. A wireless hacker uses war-driving tools to discover access points and to publish their information (MAC address, SSID, security implemented) 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 NetStumbler website (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or later versions. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas.

### 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.

WCS also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, refer to the WCS online help.

## NetStumbler Victim Detected

### 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 NetStumbler website (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or later. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers typically use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used, but from a low-flying private plane with high-power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.

### 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.

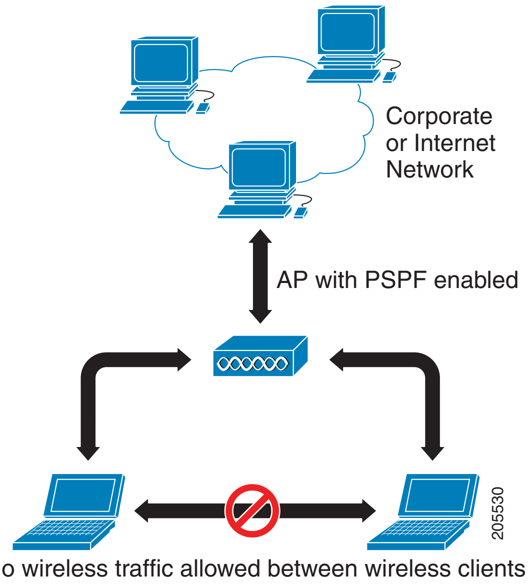
## Publicly Secure Packet Forwarding (PSPF) Violation

### Alarm Description and Possible Causes

Publicly Secure Packet Forwarding (PSPF) is a feature implemented on WLAN access points to block wireless clients from communicating with other wireless clients. With PSPF enabled, client devices cannot communicate with other client devices on the wireless network.

For most WLAN environments, wireless clients communicate only with devices such as web servers on the wired network. By enabling PSPF it protects wireless clients from being hacked by a wireless intruder. PSPF is effective in protecting wireless clients especially at wireless public networks (hotspots) such as airports, hotels, coffee shops, and college campuses where authentication is null and anyone can associate with the access points. The PSPF feature prevents client devices from inadvertently sharing files with other client devices on the wireless network (see Figure A-18).

*Figure A-18 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.

## 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 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 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.

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 WCS 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: Cqure AP

### Alarm Description and Possible Causes

A host-based access point (desktop or a laptop computer serving as a wireless access point) represents two potential threats to enterprise security. First, host based access points are not typically part of the enterprise wireless infrastructure and are likely to be rogue devices which do not conform to the corporate security policy. Second, host-based access points are used by wireless attackers as a convenient platform to implement various known intrusions such as man-in-the-middle, honey-pot access point, access point impersonation, and DoS (denial of service) attacks. 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 pre-loaded 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, refer to the *Cisco Wireless Control System Configuration Guide* or the WCS 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://www.wellenreiter.net/index.html

### wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the wIPS to see which of your access points is broadcasting an SSID in the beacons.

WCS also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, refer to the WCS online help.

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-11
- "Configuring Controller Templates" section on page B-12

## 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.

## Rogue Access Point Location, Tagging, and Containment

When the Cisco Unified Wireless Network Solution is monitored using WCS, WCS 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, WCS immediately starts listening for rogue access points. When a controller detects a rogue access point, it immediately notifies WCS, which creates a rogue access point alarm.

When WCS receives a rogue access point message from a controller, an alarm monitor appears in the lower left corner of all WCS user interface pages.

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 WCS Location, WCS compares RSSI signal strength from two or more access points to find the most probable location of the rogue access point and places a small skull-and-crossbones indicator at its most likely location. In the case of an underdeployed network for location with only one access point and an omni antenna, the most likely location is somewhere on a ring around the access point, but the center of likelihood is at the access point. If you are using WCS Base, WCS 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, 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, click **Rogue AP**.
- Click the **Malicious AP number** link in the Alarm Summary box at the bottom of the left sidebar.

**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 B-1 describes the parameters found in the Rogue Access Point Alarms page.

*Table B-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 WCS, and you can search for all Acknowledged alarms using the alarm search functionality.

- The other sections on the Rogue AP Alarms page include the following:
- 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 wish to contain any access points.

## Monitoring Rogue Access Point Details

Alarm event details for each rogue access point are available from the Rogue AP Alarms page.

To view alarm events for a rogue access point radio, from 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:
  - 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 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

Click a Rogues alarm square in the Alarm Monitor (lower left-hand side of the screen) to access the Monitor Alarms > *failure object* page. In the Monitor Rogue AP Alarms page, click an item under Rogue MAC Address to access the Monitor Alarms > Rogue AP Details page, from the Select a command drop-down list choose **Detecting APs**, and click **Go** to access this page.

Choose **Monitor > Alarms**, then click New Search in the left sidebar. Choose **Severity > All Severities and Alarm Category > Rogue AP**, and click **Go** to access Monitor Alarms > *failure object*.

In the Monitor Rogue AP Alarms page, click an item under Rogue MAC Address to access Monitor Alarms > Rogue AP Details. In the Monitor Alarms > Rogue *vendor:MACaddr* page, from the Select a command drop-down list, choose **Detecting APs** to access this page.

This page enables you to view information about the Cisco lightweight access points that are detecting a rogue access point.

Click a list item to display data about that item:

- AP Name
- Radio
- Map Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio.
- Channel Number—Which channel the rogue access point is broadcasting on.
- WEP—Enabled or disabled.
- WPA—Enabled or disabled.
- Pre-Amble—Long or short.
- RSSI—Received signal strength indicator in dBm.
- SNR—Signal-to-noise ratio.
- Containment Type—Type of containment applied from this access point.

Containment Channels—Channels that this access point is currently containing.

# Monitoring Rogue Adhoc Alarms

The Rogue Adhoc Alarms page displays alarm events for rogue adhocs.

To access the Rogue Adhoc Alarms page, do one of the following:

- Choose **Monitor > Alarms**. From the left sidebar menu, click **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, choose **Rogue Adhocs**.

**Note** If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

Table B-2 describes the parameters found in the Rogue Adhoc Alarms page.

*Table B-2 Rogue Adhoc 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 adhoc. |
| Vendor | Rogue adhoc vendor name, or Unknown. |
| Classification Type | Malicious, Friendly, or Unclassified. |
| Radio Type | Indicates the radio type for this rogue adhoc. |
| 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 adhoc. |
| Owner | Indicates the ‘owner’ of the rogue adhoc. |
| 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 adhoc radio. (Blank if SSID is not broadcast.) |
| Map Location | Indicates the map location for this rogue adhoc. |
| 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, choose one of the following commands from the Select a command drop-down list, and click **Go**.

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

- Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page.

**Note** The alarm remains in WCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the All Alarms > Email Notification page to view and configure email notifications.
- Detecting APs—View the Cisco Aironet 1000 Series lightweight access points that are currently detecting the rogue adhoc. See Detecting Access Points for more information.
- Map (High Resolution)—Click to display a high-resolution map of the rogue adhoc location.
- Rogue Clients—Click to view a list of rogue clients associated with this rogue adhoc. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the Rogue adhoc.
- Set State to 'Alert'—Choose this command to tag the rogue adhoc 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 adhoc 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 adhoc as external, add it to the Known Rogue APs list, and to turn off Containment.
- 1 AP Containment—Target the rogue adhoc for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue adhoc for containment by two Cisco Aironet 1000 Series lightweight access points.
- 3 AP Containment—Target the rogue adhoc for containment by three Cisco Aironet 1000 Series lightweight access points.
- 4 AP Containment—Target the rogue adhoc for containment by four Cisco Aironet 1000 Series lightweight access points. (Highest containment level.)

**Caution** Attempting to contain a rogue adhoc 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 wish to contain any access points.

## Monitoring Rogue Adhoc Details

Alarm event details for each Rogue adhoc are available from the Rogue Adhoc Alarms page.

To view alarm events for a rogue adhoc radio, from 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 adhoc.

  - Vendor—Rogue adhoc vendor name or Unknown.
  - On Network—Indicates whether or not the rogue adhoc 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 adhoc radio. (Blank if SSID is not broadcast.)
  - Channel Number—Indicates the channel of the rogue adhoc.
  - Containment Level—Indicates the containment level of the rogue adhoc or Unassigned.
  - Radio Type—Indicates the radio type for this rogue adhoc.
  - 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 adhoc.
  - 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 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, selecting one of the following commands, and clicking **Go**.

- Assign to me—Assign the selected alarm to the current user.
- Unassign—Unassign the selected alarm.
- Delete—Delete the selected alarm.
- Clear—Clear the selected alarm.
- Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in WCS 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 email notifications.
- Detecting APs—View the Cisco Aironet 1000 Series lightweight access points that are currently detecting the rogue adhoc. See Detecting Access Points for more information.

- Map (High Resolution)—Click to display a high-resolution map of the rogue adhoc location.
- Rogue Clients—Click to view a list of rogue clients associated with this rogue adhoc. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the Rogue adhoc.
- Set State to 'Alert'—Choose this command to tag the rogue adhoc as the lowest threat, continue monitoring the rogue adhoc, and to turn off Containment.
- Set State to 'Internal'—Choose this command to tag the rogue adhoc 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—Target the rogue adhoc for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue adhoc for containment by two Cisco Aironet 1000 Series lightweight access points.
- 3 AP Containment—Target the rogue adhoc for containment by three Cisco Aironet 1000 Series lightweight access points.
- 4 AP Containment—Target the rogue adhoc 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 click **New Search** in the left sidebar. 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 click **New Search** in 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 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 Controllers

This section contains the following topics:

- Configuring Rogue Policies, page B-11
- Configuring Rogue AP Rules, page B-12

## 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 Adhoc networks (check box)—Enabled, Disabled.Command Buttons
- Save—Save the changes made to the client exclusion policies and return to the previous page.
- Audit—Compare the WCS 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 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 "Configuring Rogue AP Rules" section on page B-13 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 adhoc 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. From the Apply to Controllers screen, 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. WCS 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** Enter the following parameters:

- 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.

**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.

**Note** User Configured SSID are the SSIDs that are manually added. Enter the User Configured SSIDs (one per line) in the text box below Match User Configured SSID.

  - 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 screen, 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 section. See Configuring Rogue AP Rules, page B-13 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.

APPENDIX C

# Radio Resource Management

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.

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.

WCS 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 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 difference 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 WCS 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 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 points' 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 WCS 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 dashboard includes the following:

- The RRM Statistics portion shows network-wide statistics.
- The Channel Change Reason portion shows why channels changed for all 802.11a/b/g/n radios.
- The Channel Change shows all events complete with causes.
- The Configuration Mismatch portion shows comparisons between the leaders and members.
- The Coverage Hole portion rates how severe the coverage holes are and gives their location.
- The Percent Time at Maximum Power shows what percent of time the access points were at maximum power and gives the location of those access points.

The following statistics are displayed:

- Total Channel Changes—The sum total of channel changes across 802.11a/b/g/n radios, irrespective of whether the channel was updated or revised. The count is split over a 24-hour and 7-day period. If you click the percentages link or the link under the 24-hour column, a screen 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 WCS.
- 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 on the desired radio in the Radio column.

**Step 5** Choose 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 to select a template name in the Template Name column. The 802.11a/n or 802.11b/g/n RRM Thresholds Template 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** At the RF Utilization parameter, 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 WCS.

**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 between 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 amongst 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 from 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**.

APPENDIX D

# MSE System and Appliance Hardening Guidelines

This appendix describes the hardening of MSE, which requires some services and processes to be exposed to function properly. In other words is referred to as MSE Appliance Best Practices. Hardening of MSE involves disabling unnecessary services, upgrading to the latest server versions, and applying appropriate restrictive permissions to files, services, and end points.

This appendix contains the following sections:

- Setup Wizard Update, page D-1
- Certificate Management, page D-2
- WCS GUI Updates for SNMPv3, page D-10
- Updated Open Port List, page D-10
- Syslog Support, page D-10
- MSE and RHEL 5, page D-11

## Setup Wizard Update

The following configuration options have been included in the Setup.sh script:

- Configure future restart day and time, page D-1
- Configure Remote Syslog Server to publish MSE logs, page D-2
- Configure Host access control settings, page D-2

### Configure future restart day and time

Use this option if you want to specify the day and time when you want the MSE to restart. If you do not specify anything then Saturday 1 AM is taken as default.

**Example:**

```
Configure future restart day and time ? (Y)es/(S)kip [Skip]:
```

## Configure Remote Syslog Server to publish MSE logs

Use this option to configure a Remote Syslog Server by specifying the IP address, priority parameter, priority level, and facility.

**Example:**

```
A Remote Syslog Server has not been configured for this machine.
Configure Remote Syslog Server Configuration parameters? (Y)es/(S)kip/(U)se default
[Skip]: y
Configure Remote Syslog Server IP address: 283.12.13.4

Configure Remote Syslog Server Priority parameter.
select a priority level
1)ERROR (ERR)
2)WARNING
3)INFO
Enter a priority level (1-3) :2
Configure Remote Syslog Server's Facility parameter.
Select a logging facility
0) LOCAL0 (16)
1) LOCAL1 (17)
2) LOCAL2 (18)
3) LOCAL3 (19)
4) LOCAL4 (20)
5) LOCAL5 (21)
6) LOCAL6 (22)
7) LOCAL7 (23)
Enter a facility(0-7) :4
```

## Configure Host access control settings

You can use this option to add or delete or clear the hosts for accessing the MSE.

**Example:**

```
Enter whether or not you would like to change the iptables for this machine (giving access
to certain host).
Configure Host access control settings ? (Y)es/(S)kip [Skip]: y
Choose to add/delete/clear host for access control(add/delete/clear): add
Enter IP address of the host / subnet for access to MSE : 258.19.35.0/24
```

For more information on the setup.sh script, see *Cisco 3350 Mobility Services Engine Getting Started Guide*.

# Certificate Management

Currently MSE ships with self generated certificates. For establishing the trust in SSL connection establishment, MSE either uses a valid Cisco certificate authority (CA) issued certificate or allows importing a valid CA issued server certificate. To accomplish this, a CLI based CertMgmt.sh is used to import Server and CA certificates.

To access the CertMgmt.sh script file, go to the following folder:

/opt/mse/framework/bin/

You can do the following using the CertMgmt.sh script:

- Create a CSR, page D-3
- Import CA Certificate, page D-4
- Import Server Certificate, page D-4
- Enable or Disable Client Certificate Validation, page D-5
- OCSP Settings, page D-5
- Import a CRL, page D-6
- Clear Certificate Configuration, page D-6
- Show Certificate Configuration, page D-7

## Create a CSR

Use this option to create a Certificate Signing Request. The output of this request is the Server Certificate Signing Request and Key. You need to copy the Server CSR and paste it into the certificate authority's website to generate a CA certificate.

**Example:**

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
7
Enter the directory in which the CSR needs to be stored:/root/TestFolder
Enter the Keysize: 2048
Generating a 2048 bit RSA private key
..........................................................+++
.........+++
writing new private key to '/root/TestFolder/mseserverkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
Verify failure
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:IN
State or Province Name (full name) [Berkshire]:State
Locality Name (eg, city) [Newbury]:City
Organization Name (eg, company) [My Company Ltd]:xyz
Organizational Unit Name (eg, section) []:ABCD
Common Name (eg, your name or your server's hostname) []:example-mse
Email Address []:user@example.com
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:password123
An optional company name []:abc
The CSR is in: /root/TestFolder/mseservercsr.pem
The Private key is in: /root/TestFolder/mseserverkey.pem
```

# Import CA Certificate

The Certificate Authority sends the CA certificate based on the Server CSR and the Private Key you submitted.

Use the `Import CA Certificate` option to import a CA certificate.

**Example:**

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
1
Do you want to file(0) or scp(1) transfer (0/1) 0
Enter the full path of the CA certificate file /root/TestFolder/CACert.cer
Successfully transferred the file
Import CA Certificate successful
```

# Import Server Certificate

After obtaining the CA certificate, you need to obtain the Server Certificate. Then you need to append the Private Key information toward the end of the Server Certificate.

Use the `Import Server Certificate` option to import a server certificate.

**Example:**

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
2
Do you want to file(0) or scp(1) transfer (0/1) 0
Enter the full path of the server certificate file /root/TestFolder/ServerCertUpdated.cer
```

```
Successfully transferred the file
Enter pass phrase for /var/mse/certs/exportCert.cer:
Enter Export Password:
Verifying - Enter Export Password:
Enter password for PKCS12 file:
pk12util: PKCS12 IMPORT SUCCESSFUL
Validation is Successful
Import Server Certificate successful
```

## Enable or Disable Client Certificate Validation

The CA certificate that you obtain from the certificate authority is also copied to the associated clients.

Use this option to enable or disable client certificate validation.

**Example:**

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
3
Enabling client certificate validation done

Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
3
Enabling client certificate validation done
```

## OCSP Settings

Use this option to configure the Online Certificate Status Protocol (OCSP) settings. You are prompted to enter the OCSP URL and default name. In other words, you are asked to provide the URL and default name for the certificate authority.

**Example:**

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
5
Enter the OCSP URL :
http://ocsp.227.104.178.224
Enter the default ocsp name :ExampleServer
```

# Import a CRL

Use this option to import a Certificate Revokation List (CRL) which you have obtained from the website of the certificate authority.

**Example:**

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
6
Do you want to file(0) or scp(1) transfer (0/1) 0
Enter the full path of the CRL file /root/TestFolder/Sample.crl
Successfully transferred the file
Import CRL successful
```

# Clear Certificate Configuration

Use this option to clear the certificate configurations.

**Example:**

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
```

```
Please enter your choice (1-10)
8
httpd (no pid file) not running
Flushing firewall rules: [  OK  ]
Setting chains to policy ACCEPT: filter [  OK  ]
Unloading iptables modules: [  OK  ]
```

## Show Certificate Configuration

Use this option to display the certificate details.

**Example:**

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
9

Certificate Nickname                                         Trust Attributes
                                                             SSL,S/MIME,JAR/XPI

CA-Cert1296638915                                            CT,,
Server-Cert                                                  u,u,u
=========================================================
*************************  Certificates in the database  ********************
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            74:a1:38:25:75:94:a5:9a:43:2d:4a:23:bd:82:bc:e5
        Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
        Issuer: "CN=ROOTCA1"
        Validity:
            Not Before: Tue Nov 16 18:49:25 2010
            Not After : Mon Nov 16 18:59:25 2015
        Subject: "CN=ROOTCA1"
        Subject Public Key Info:
            Public Key Algorithm: PKCS #1 RSA Encryption
            RSA Public Key:
                Modulus:
                    da:06:43:70:56:d8:41:ec:69:e6:65:ad:c5:3b:04:0b:
                    cb:cd:83:7c:5f:6e:8f:aa:17:50:6b:6a:3a:48:35:a6:
                    65:8a:47:91:48:2f:93:2b:d8:53:6b:33:5c:a9:c2:b2:
                    33:c2:fc:9c:55:25:19:d0:79:23:3f:66:60:24:04:ce:
                    a3:08:c7:60:f0:b0:8d:b1:31:71:f5:b9:3f:17:46:1a:
                    fd:3d:c9:3b:9f:bf:fe:a3:8d:13:52:aa:6b:59:80:43:
                    f8:24:e7:49:10:ca:54:6c:f7:aa:77:04:4b:c2:3f:96:
                    8d:a1:46:e8:16:1e:a8:e6:86:f4:5c:a0:e5:15:eb:f8:
                    5a:72:97:f9:09:65:84:f6:a5:0b:a3:c6:ab:a9:9e:61:
                    07:5a:8d:b1:af:93:3b:68:53:8a:5d:f0:14:6e:02:e4:
                    38:d2:31:29:5e:a2:1a:93:de:a0:bd:44:9b:05:fd:7b:
                    5f:59:23:a1:47:97:87:84:dd:0e:9f:0a:09:cd:df:34:
```

```
                    b9:6f:9c:b5:4d:07:23:8b:a5:27:16:cd:75:5a:6e:f1:
                    c1:5b:6b:21:3a:fd:d9:4d:72:b4:d6:dc:37:86:c2:e3:
                    60:56:69:3c:52:27:19:bf:4c:0c:ea:6e:34:29:8c:cf:
                    17:50:b3:31:cc:86:1e:32:dc:40:58:92:26:88:58:63
                Exponent: 65537 (0x10001)
        Signed Extensions:
            Name: Certificate Key Usage
            Usages: Digital Signature
                    Certificate Signing
                    CRL Signing

            Name: Certificate Basic Constraints
            Critical: True
            Data: Is a CA with no maximum path length.

            Name: Certificate Subject Key ID
            Data:
                30:89:49:06:62:fe:6c:29:75:bc:90:8b:a5:6a:87:f8:
                8e:61:49:eb

            Name: Microsoft CertServ CA version
            Data: 0 (0x0)

    Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
    Signature:
        d6:35:b9:27:1f:5b:1a:12:9d:41:a3:16:3a:3a:08:ba:
        91:f4:a9:4b:1b:ff:71:7c:4e:74:16:36:05:04:37:27:
        d0:73:66:a2:47:50:0d:b3:fa:b1:34:dc:36:b8:a9:0a:
        2d:5c:84:35:30:51:4f:7b:55:47:00:53:73:40:c8:95:
        a9:82:83:32:06:ed:0c:95:6d:b1:13:08:3a:e3:cc:88:
        40:9f:e6:43:8c:36:88:e4:a1:91:3e:20:74:29:bf:91:
        25:c1:ef:bc:10:bb:cb:be:08:2c:64:2d:41:a1:3f:81:
        48:ed:80:ed:97:68:6d:83:30:e2:c8:90:ce:45:3a:45:
        cc:78:3c:c4:af:62:73:6a:29:60:c7:70:b1:4c:84:43:
        77:2d:9c:b9:13:dc:9c:b5:8c:74:62:7b:8e:41:ed:37:
        b8:2c:c0:3b:0c:49:cf:61:40:cc:2c:22:74:b2:6b:50:
        e8:31:c9:5f:b8:04:dd:39:7a:9a:46:5e:ee:5a:e8:6a:
        4b:75:97:69:7e:fc:7f:9d:9f:df:f0:3f:06:62:79:77:
        d9:a8:49:a6:00:bf:93:61:00:aa:55:11:26:92:f4:c2:
        8a:61:21:80:af:ef:ab:22:11:ee:10:79:15:4b:1a:8f:
        ae:55:c5:61:03:8e:db:1a:3e:5a:6f:a6:6d:3e:5b:a4
    Fingerprint (MD5):
        31:54:A0:D3:A7:40:1A:1E:95:8E:8A:D9:EC:70:47:35
    Fingerprint (SHA1):
        F5:72:62:5C:46:AB:2A:5D:7A:75:DA:CB:44:E6:38:76:E0:9E:17:C3

    Certificate Trust Flags:
        SSL Flags:
            Valid CA
            Trusted CA
            Trusted Client CA
        Email Flags:
        Object Signing Flags:

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            4d:a9:34:de:00:00:00:00:00:0b
        Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
        Issuer: "CN=ROOTCA1"
        Validity:
            Not Before: Wed Feb 02 22:40:44 2011
            Not After : Thu Feb 02 22:50:44 2012
    Subject: "E=abc@example.com,CN=abc-mse,OU=XYZ,O=Companyo,L=City,S
        T=State,C=IN"
    Subject Public Key Info:
        Public Key Algorithm: PKCS #1 RSA Encryption
        RSA Public Key:
            Modulus:
                a8:7b:2f:57:94:53:fc:90:c9:37:cb:9a:b3:f6:f4:b8:
                02:04:f3:f8:d8:e1:d1:23:d4:62:7b:30:05:d2:b0:da:
                17:88:b0:22:d5:a6:04:c6:66:fc:64:54:ff:78:5b:f9:
                ef:05:3a:3e:ec:b8:01:7c:3c:9b:78:ac:1d:7f:fb:3b:
                39:f5:31:d2:a2:27:d8:d1:ee:2e:77:98:04:bb:7c:f6:
                0b:9c:ea:15:12:cf:3d:1c:b8:57:63:df:2b:00:48:25:
                32:e4:58:9a:e1:ff:80:5d:2c:24:75:e2:06:de:e6:ae:
                03:7e:c5:f6:e7:97:4d:c1:ad:19:4f:47:20:6c:8d:7a:
                60:75:85:34:3e:ed:f3:1a:77:65:e2:7a:18:e1:17:3d:
                bd:62:1a:1c:4a:d9:49:c3:93:2e:6a:69:fc:e8:87:1e:
                dc:69:11:63:f1:17:63:41:e4:8d:1e:19:3c:e8:80:a9:
                6b:04:c8:18:fb:c9:fe:9d:77:71:30:d2:87:46:82:49:
                0a:1d:ed:4d:ad:66:ad:65:6f:fb:b2:6a:31:45:33:59:
                a7:04:3a:2d:72:f7:55:02:fa:99:02:d9:dd:5e:21:4b:
                2c:c9:3e:cc:a4:a0:dd:4c:4f:7f:be:45:a7:dd:a9:c4:
                ad:bc:a9:25:a6:1f:53:b8:d0:98:4a:b7:c3:41:a3:d7
            Exponent: 65537 (0x10001)
    Signed Extensions:
        Name: Certificate Subject Key ID
        Data:
            bc:a3:66:c6:19:07:56:0a:90:7a:b1:1a:ea:37:17:20:
            74:b8:f1:f5

        Name: Certificate Authority Key Identifier
        Key ID:
            30:89:49:06:62:fe:6c:29:75:bc:90:8b:a5:6a:87:f8:
            8e:61:49:eb

        Name: CRL Distribution Points
        URI: "http://win-bncnizib5e2/CertEnroll/ROOTCA1.crl"
        URI: "file://WIN-BNCNIZIB5E2/CertEnroll/ROOTCA1.crl"

        Name: Authority Information Access
        Method: PKIX CA issuers access method
        Location:
            URI: "http://win-bncnizib5e2/CertEnroll/WIN-BNCNIZIB5E2_ROOTC
                A1.crt"
        Method: PKIX CA issuers access method
        Location:
            URI: "file://WIN-BNCNIZIB5E2/CertEnroll/WIN-BNCNIZIB5E2_ROOTC
                A1.crt"

Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
Signature:
    aa:13:74:0d:d1:8c:85:cc:3d:8f:35:c7:e5:9b:a6:4c:
    f8:8b:12:a0:12:9f:dc:0a:0a:b5:40:12:eb:05:a9:2b:
    65:c5:a3:22:62:1f:47:cd:dd:0f:b8:03:11:a5:63:23:
    64:a7:f8:8b:ec:d4:21:dc:d8:22:de:52:75:d9:fb:23:
    d4:14:35:d8:78:b7:e2:23:75:05:b4:d0:09:e0:55:ec:
    96:8c:22:23:fb:86:74:71:69:ac:03:57:b6:ec:14:a9:
    f9:99:b3:98:4c:00:69:e2:26:f8:7b:e9:a0:2a:c2:f4:
    6a:75:fc:d1:08:d6:5b:76:93:7a:2c:21:8b:83:ab:52:
    a0:85:16:f1:38:35:01:8d:21:34:60:b7:82:39:a7:42:
    e7:5f:1a:b7:9d:bf:54:ee:27:97:ba:f8:ca:31:d4:35:
    67:55:36:02:b4:48:ab:16:ee:0f:65:56:48:51:de:aa:
    9f:7d:35:9b:eb:58:3a:0c:4a:8a:ae:3a:18:47:e3:11:
    7b:82:b3:fb:88:94:df:85:82:23:0b:07:46:12:2c:d0:
    dd:a7:91:c0:e1:4c:e7:38:9e:34:30:9b:b6:db:c6:8d:
        03:df:6e:6b:27:76:da:31:50:44:cd:c8:21:30:42:3c:
        75:dc:99:d2:6b:91:9e:bd:b0:5c:8a:52:6b:92:41:0f
    Fingerprint (MD5):
        77:73:3C:D6:B9:2E:F2:AA:C4:A6:7E:9F:60:D7:55:F7
    Fingerprint (SHA1):
        60:F8:DC:D2:75:BA:D9:35:4D:21:60:CA:90:EF:09:67:FF:D0:DC:CF

    Certificate Trust Flags:
        SSL Flags:
            User
        Email Flags:
            User
        Object Signing Flags:
            User

******************************  CRLs in the database  ***********************
None
*******************  Client Certification Settings  ****************************
Client Certificate Validation is disabled
******************************  OCSP Setting  *********************************
OCSP URL :
http://ocsp.227.104.178.224
OCSP nick name :ExampleServer
=========================================================
```

# WCS GUI Updates for SNMPv3

For more information on SNMPv3 related GUI changes, see the following:

- Adding an Event Definition, page 6-3
- Adding Trap Destinations, page 4-8

# Updated Open Port List

As part of the non-user requirement, MSE listens on HTTP (8880) and HTTP (8843) ports.

The following are the open port list for MSE:

| | |
|---|---|
| TCP | 80, 443, 22, 8001 |
| | 4096, 1411, 4000X (x=1,5) |
| UDP | 162, 12091, 12092 |

# Syslog Support

To ensure compliance to DoD requirement, wIPS supports Syslog messaging.

# MSE and RHEL 5

The MSE OS is based on RHEL (Red Hat Enterprise Linux) 5 and the current version of RHEL supported by MSE OS is 5.4. If you are using RHEL 5.3 or earlier, then download and update the openssl patches. Upgrade to RHEL5.4 supports OpenSSH version 4.3p2-36.el5 (which addresses the vulnerabilities in 4.3p2-26.el5_2.1).

# INDEX

A

alarm notifications
    emailing 7-6
alarms
    assigning 7-5
    clearing 7-6
    deleting 7-6
    unassigning 7-5
    viewing 7-2
audit report
    for alarms 7-4
automatic synchronization 3-5

C

certificate management D-2

E

event history 7-5
events
    viewing 7-8

G

general properties
    editing 4-1
groups
    adding 5-1
    deleting 5-2
    permissions 5-2

L

location server
    backup historical data 8-2
    restore historical data 8-3
    software download 8-4
log files
    download 7-10
log options
    configuring 7-9

M

monitor alarms
    Rogue B-8
    Rogue APs B-7

N

network designs 3-1
NTP Server
    Configuring 8-6

O

out-of-sync 3-7

P

password
    recovering lost 8-1

R

rogue policies
  templates B-12

S

scheduled tasks 3-6
synchronization 3-7
synchronization history 3-8
synchronization status 3-7
system and appliance hardening D-1

T

templates
  controller
    rogue policies B-12

U

users
  adding 5-3
  deleting 5-4
  properties 5-4