



Cisco Context-Aware Service Configuration Guide

Release 7.3
August 2012

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

Text Part Number: OL-23943-02

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

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

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

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

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

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

Cisco Context-Aware Service Configuration Guide
Copyright © 2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xv

- Objectives xv
- Audience xv
- Conventions xv
- Related Documentation xvi
- Obtaining Documentation and Submitting a Service Request xvi

CHAPTER 1

Overview 1-1

- About the Cisco Context-Aware Mobility Solution 1-1
 - Cisco 3300 Series Mobility Services Engines 1-1
 - CAS 1-2
- Licensing Information for Clients and Tags 1-2
- Guidelines and Limitations 1-3
- Viewing Contextual Information 1-3
 - ContextAware Tab 1-3
 - Location Assisted Client Troubleshooting from the ContextAware Dashboard 1-4
- Event Notification 1-5
- Configuration and Administration 1-6
 - Adding and Deleting a Mobility Services Engine 1-6
 - Synchronizing Mobility Services Engines 1-6
 - Configuring High Availability 1-6
 - Configuring the Virtual Appliance 1-7
 - Editing Mobility Services Engine Properties 1-7
 - Managing Users and Groups 1-7
 - Configuring Event Notifications 1-7
 - Context-Aware Planning and Verification 1-7
 - Working with Maps 1-7
 - Monitoring Capability 1-8
 - Provisioning MSAP Requirements 1-8
 - Maintenance Operations 1-8
 - MSE System and Appliance Hardening 1-8
 - System Compatibility 1-8

CHAPTER 2

Adding and Deleting Mobility Services Engines and Licenses 2-1

- Licensing Requirements for MSE 2-1
 - MSE License Structure Matrix 2-2
 - Sample MSE License File 2-2
 - Revoking and Reusing an MSE License 2-2
 - Revoking an MSE License Using the MSE CLI 2-3
- Guidelines and Limitations 2-3
- Adding a Mobility Services Engine to the Prime Infrastructure 2-4
 - Deleting an MSE License File 2-7
 - Deleting a Mobility Services Engine from the Prime Infrastructure 2-7
- Registering Device and wPS Product Authorization Keys 2-8
- Installing Device and wPS License Files 2-12
- Registering Tag PAKs 2-12
- Installing Tag Licenses 2-13

CHAPTER 3

Synchronizing Mobility Services Engines 3-1

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

CHAPTER 4

Configuring High Availability 4-1

- Overview to the High Availability Architecture 4-1
- Pairing Matrix 4-2
- Guidelines and Limitations for High Availability 4-2

Failover Scenario for High Availability	4-2
Failback	4-3
HA Licensing	4-3
Configuring High Availability on the MSE	4-3
Viewing Configured Parameters for High Availability	4-6
Viewing High Availability Status	4-7

CHAPTER 5

MSE Delivery Modes	5-1
Physical Appliance	5-1
Virtual Appliance	5-1
Operating Systems Requirements	5-2
Client Requirements	5-2
Prerequisites for Setting Up an MSE Virtual Appliance on a Server	5-3
Virtual Appliance Sizing	5-3
Reinstalling the MSE on a Physical Appliance	5-3
Deploying the MSE Virtual Appliance	5-4
Deploying the MSE Virtual Appliance from the VMware vSphere Client	5-4
Configuring the Basic Settings to Start the MSE Virtual Appliance VM	5-7
Deploying the MSE Virtual Appliance Using the Command-Line Client	5-8
Adding a Virtual Appliance License to the Prime Infrastructure	5-8
Adding a License File to the MSE Using the License Center	5-8
Viewing the MSE License Information Using the License Center	5-9
Removing a License File Using the License Center	5-9

CHAPTER 6

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

Rebooting or Shutting Down a System 6-9
 Clearing the System Database 6-9

CHAPTER 7

Managing Users and Groups 7-1

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

CHAPTER 8

Configuring Event Notifications 8-1

Information About Event Notifications 8-1
 Viewing Event Notification Summary 8-2
 Clearing Notifications 8-2
 Notification Message Formats 8-3
 Notification Formats in XML 8-3
 Missing (Absence) Condition 8-3
 In/Out (Containment) Condition 8-4
 Distance Condition 8-4
 Battery Level 8-5
 Location Change 8-5
 Chokepoint Condition 8-5
 Emergency Condition 8-5
 Notification Formats in Text 8-6
 The Prime Infrastructure as a Notification Listener 8-6
 Guidelines and Limitations 8-7
 Adding and Deleting Event Groups 8-7
 Adding Event Groups 8-7
 Deleting Event Groups 8-7
 Adding, Deleting, and Testing Event Definitions 8-8
 Adding an Event Definition 8-8
 Defining a Chokepoint 8-10
 Deleting an Event Definition 8-12

Testing Event Definitions	8-12
Viewing Event Notification Summary	8-12

CHAPTER 9

Context-Aware Service Planning and Verification	9-1
Licensing Requirements	9-1
Guidelines and Limitations	9-2
Planning Data, Voice, and Location Deployment	9-2
Guidelines and Limitations	9-2
Calculating the Placement of Access Points	9-2
Calibration Models	9-3
Information on Calibration Models	9-3
Guidelines and Limitations	9-3
Creating and Applying Data Point and Calibration Models	9-4
Inspecting Location Readiness and Quality	9-7
Guidelines and Limitations	9-7
Inspecting Location Readiness Using Access Point Data	9-7
Inspecting Location Quality Using Calibration Data	9-8
Verifying Location Accuracy	9-8
Using Scheduled Accuracy Testing to Verify Current Location Accuracy	9-9
Using On-Demand Location Accuracy Testing	9-10
Using Optimized Monitor Mode to Enhance Tag Location Reporting	9-12
Guidelines and Limitations	9-12
Optimizing Monitoring and Location Calculation of Tags	9-12
Defining Inclusion and Exclusion Regions on a Floor	9-13
Guidelines and Limitations	9-13
Opening the Map Editor	9-13
Using the Map Editor to Draw Coverage Areas	9-14
Defining an Inclusion Region on a Floor	9-14
Defining an Exclusion Region on a Floor	9-16
Defining a Rail Line on a Floor	9-17
Guidelines and Limitations	9-17
Defining a Rail on a Floor	9-18
Adding an Outdoor Area	9-18
Configuring Interferer Notifications	9-19
Using Planning Mode	9-20
Modifying Context-Aware Service Parameters	9-21
Licensing Requirements	9-21
Guidelines and Limitations	9-22

- Modifying Tracking Parameters 9-22
 - Guidelines and Limitations 9-22
 - Configuring Tracking Parameters for a Mobility Services Engine 9-22
- Modifying Filtering Parameters 9-26
 - Guidelines and Limitations 9-26
 - Configuring Filtering Parameters for a Mobility Services Engine 9-26
- Modifying History Parameters 9-28
 - Configuring Mobility Services Engine History Settings 9-29
- Enabling Location Presence 9-30
 - Guidelines and Limitations 9-30
 - Enabling and Configuring Location Presence on a Mobility Services Engine 9-30
- Importing and Exporting Asset Information 9-31
 - Importing Asset Information 9-31
 - Exporting Asset Information 9-32
- Modifying Location Parameters 9-32
 - Guidelines and Limitations 9-32
 - Configuring Location Parameters 9-32
- Enabling Notifications and Configuring Notification Parameters 9-35
 - Guidelines and Limitations 9-35
 - Enabling Notifications 9-35
 - Configuring Notification Parameters 9-35
 - Viewing Notification Statistics 9-37
- Location Template for Controllers 9-38
 - Configuring a New Location Template for a Controller 9-38
- Location Services on Wired Switches and Wired Clients 9-40
 - Prerequisites to Support Location Services for Wired Clients 9-41
 - Guidelines and Limitations 9-41
 - Configuring a Catalyst Switch Using the CLI 9-41
 - Adding a Catalyst Switch to the Prime Infrastructure 9-43
 - Assigning and Synchronizing a Catalyst Switch to a Mobility Services Engine 9-43
- Verifying an NMSP Connection to a Mobility Services Engine 9-44

CHAPTER 10

Working with Maps 10-1

- About Maps 10-1
 - Adding a Campus Map 10-2
 - Adding a Building to a Campus Map 10-2
 - Adding a Standalone Building 10-4
- Adding Floor Areas 10-5
 - Adding Floor Areas to a Campus Building 10-5

Adding Floor Plans to a Standalone Building	10-8
Monitoring the Floor Area	10-10
Panning and Zooming with Next Generation Maps	10-11
Adding Access Points to a Floor Area	10-11
Placing Access Points	10-14
Using the Automatic Hierarchy to Create Maps	10-15
Using the Map Editor	10-17
Guidelines for Using the Map Editor	10-17
Guidelines for Inclusion and Exclusion Areas on a Floor	10-18
Opening the Map Editor	10-18
Map Editor Icons	10-19
Using the Map Editor to Draw Coverage Areas	10-19
Using the Map Editor to Draw Obstacles	10-20
Map Editor Edit Mode	10-20
Defining an Inclusion Region on a Floor	10-21
Defining an Exclusion Region on a Floor	10-22
Defining a Rail Line on a Floor	10-23
Adding an Outdoor Area	10-24
Using Planning Mode	10-25
Using Chokepoints to Enhance Tag Location Reporting	10-25
Guidelines and Limitations	10-26
Adding Chokepoints to the Prime Infrastructure	10-26
Adding a Chokepoint to a Prime Infrastructure Map	10-27
Positioning Chokepoints	10-28
Removing Chokepoints from the Prime Infrastructure	10-29
Configuring Wi-Fi TDOA Receivers	10-29
Prerequisites for Using TDOA Receiver Within the Cisco Unified Wireless Network	10-29
Adding Wi-Fi TDOA Receivers to the Prime Infrastructure Database	10-30
Adding Wi-Fi TDOA Receivers to a Map	10-30
Positioning Wi-Fi TDOA Receivers	10-31
Removing Wi-Fi TDOA Receivers from the Prime Infrastructure	10-31

CHAPTER 11**Monitoring the System and Services 11-1**

Working with Alarms	11-1
Guidelines and Limitations	11-1
Viewing Alarms	11-2
Viewing the MSE Alarm Details	11-2
Assigning and Unassigning Alarms	11-4
Deleting and Clearing Alarms	11-5

- E-mailing Alarm Notifications 11-5
- Working with Events 11-6
 - Displaying Location Notification Events 11-6
- Working with Logs 11-6
 - Guidelines and Limitations 11-6
 - Configuring Logging Options 11-7
 - MAC Address-based Logging 11-8
 - Downloading Log Files 11-8
- Generating Reports 11-8
 - Report Launch Pad 11-9
 - Creating and Running a New Report 11-9
 - Managing Current Reports 11-15
 - Managing Scheduled Run Results 11-15
 - Managing Saved Reports 11-16
- Generating MSE Analytics Reports 11-18
 - Client Location 11-18
 - Configuring a Client Location Report 11-19
 - Client Location Results 11-19
 - Client Location Density 11-20
 - Configuring a Client Location Density Report 11-20
 - Client Location Density Results 11-21
 - Device Count by Zone 11-21
 - Configuring a Device Count by Zone Report 11-22
 - Device Count by Zone Results 11-23
 - Device Dwell Time by Zone 11-23
 - Configuring a Device Dwell Time by Zone Report 11-23
 - Device Dwell Time by Zone Results 11-24
 - Guest Location Density 11-25
 - Configuring Guest Location Tracking 11-25
 - Guest Location Tracking Results 11-26
 - Location Notifications by Zone 11-26
 - Configuring a Location Notification Report 11-26
 - Location Notification Results 11-28
 - Mobile MAC Statistics 11-28
 - Configuring Mobile MAC Statistics 11-28
 - Mobile MAC Statistics 11-29
 - Rogue AP Location Density 11-29
 - Configuring Rogue AP Location Tracking 11-30
 - Rogue Client Location Density 11-31

Configuring a Rogue Client Location Tracking	11-31
Rogue Client Location Tracking Results	11-32
Tag Location	11-32
Configuring Tag Location History	11-33
Tag Location Density	11-34
Tag Location Tracking Results	11-35
Creating a Device Utilization Report	11-35
Viewing Saved Utilization Reports	11-37
Viewing Scheduled Utilization Runs	11-38
Managing OUI	11-38
Adding a New Vendor OUI Mapping	11-38
Uploading an Updated Vendor OUI Mapping File	11-39
Monitoring Wireless Clients	11-39
Monitoring Wireless Clients Using Maps	11-39
Monitoring Wireless Clients Using Search	11-40
Client Support on the MSE	11-41
Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address	11-42
Viewing the Clients Detected by the MSE	11-43
Configuring Buildings	11-48
Adding a Building to a Campus Map	11-49
Viewing a Building	11-51
Editing a Building	11-52
Deleting a Building	11-52
Moving a Building	11-53
Monitoring Tags	11-53
Monitoring Tags Using Maps	11-53
Monitoring Tags Using Search	11-54
Overlapping Tags	11-57
Monitoring Chokepoints	11-57
Monitoring Wi-Fi TDOA Receivers	11-58
Monitoring Geo-Location	11-59
Adding a GPS Marker to a Floor Map	11-60
Editing a GPS Marker	11-60
Deleting a GPS Marker Present on a Floor	11-61
Ekahau Site Survey Integration	11-61
AirMagnet Survey and Planner Integration	11-62
Monitoring Wired Switches	11-62
Monitoring Wired Clients	11-63

- Monitoring Interferers 11-64
 - Monitor > Interferers > AP Detected Interferers 11-64
 - Monitor > Interferers > AP Detected Interferers > Interferer Details 11-65
 - Monitor > Interferers > AP Detected Interferer Details > Interference Device ID > Location History 11-66
 - Monitor > Interferers > Edit View 11-67
 - Clustering of Monitor Mode APs Using the MSE 11-69

CHAPTER 12

MSAP

- 12-1
 - Licensing for MSAP 12-1
 - Provisioning MSAP Service Advertisements 12-2
 - Adding Service Advertisements to the Floor Map 12-3
 - Creating Service Advertisements from the Floor Map 12-4
 - Deleting Service Advertisements 12-4
 - Applying Service Advertisements to a Venue 12-4
 - Viewing the Configured Service Advertisements per MSE 12-5
 - Viewing MSAP Statistics 12-5
 - Viewing the MSE Summary Page for MSAP License Information 12-6
 - Viewing Service Advertisements Synchronization Status 12-6
 - MSAP Reports 12-6
 - Mobile MAC Statistics 12-6
 - Service URI Statistics 12-7

CHAPTER 13

Performing Maintenance Operations

- 13-1
 - Guidelines and Limitations 13-1
 - Recovering a Lost Password 13-1
 - Recovering a Lost Root Password 13-2
 - Backing Up and Restoring Mobility Services Engine Data 13-2
 - Guidelines and Limitations 13-2
 - Backing Up Mobility Services Engine Historical Data 13-3
 - Restoring Mobility Services Engine Historical Data 13-3
 - Enabling Automatic Location Data Backup 13-4
 - Downloading Software to the Mobility Services Engines 13-4
 - Manually Downloading Software 13-5
 - Configuring the NTP Server 13-6
 - Resetting the System 13-6
 - Clearing the Configuration File 13-7

APPENDIX A**MSE System and Appliance Hardening Guidelines A-1**

- Setup Wizard Update **A-1**
 - Configuring Future Restart Day and Time **A-1**
 - Configuring the Remote Syslog Server to Publish MSE Logs **A-2**
 - Configuring the Host Access Control Settings **A-2**
- Certificate Management **A-2**
 - Creating a CSR **A-3**
 - Importing the CA Certificate **A-4**
 - Importing the Server Certificate **A-4**
 - Enabling or Disabling Client Certificate Validation **A-5**
 - Configuring OCSP Settings **A-5**
 - Importing a CRL **A-6**
 - Clearing Certificate Configuration **A-6**
 - Showing Certificate Configuration **A-7**
- Prime Infrastructure GUI Updates for SNMPv3 **A-10**
- Updated Open Port List **A-10**
- Syslog Support **A-10**
- MSE and RHEL 5 **A-11**

INDEX



Preface

This preface contains the following sections:

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

Objectives

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

Audience

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

Conventions

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

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

Examples use the following conventions:

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

**Note**

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

**Tip**

Means the following information will help you solve a problem.

**Caution**

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

Related Documentation

See the *Cisco 3310 Mobility Services Engine Getting Started Guide* or *Cisco 3350 Mobility Services Engine Getting Started Guide* for mobility services engine installation and setup information.

These documents are available on Cisco.com at the following URL:

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

Obtaining Documentation and Submitting a Service Request

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

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

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



CHAPTER 1

Overview

This chapter describes the role of the Cisco 3300 series mobility services engine (MSE), a component of the Cisco Context-Aware Mobility (CAM) solution, within the overall Cisco Unified Wireless Network (CUWN).

Additionally, Context-Aware Service (CAS) software, a service supported on the mobility services engine and a component of the CAM, is addressed.

This chapter contains the following sections:

- [About the Cisco Context-Aware Mobility Solution, page 1-1](#)
- [Licensing Information for Clients and Tags, page 1-2](#)
- [Guidelines and Limitations, page 1-3](#)
- [Viewing Contextual Information, page 1-3](#)
- [Event Notification, page 1-5](#)
- [Configuration and Administration, page 1-6](#)

About the Cisco Context-Aware Mobility Solution

The foundation of the CAM solution is the controller-based architecture of the CUWN. The CUWN contains the following primary components: access points, wireless LAN controllers, the Cisco Prime Infrastructure management application, and the Cisco 3300 series mobility services engine.

This section contains the following topics:

- [Cisco 3300 Series Mobility Services Engines, page 1-1](#)
- [CAS, page 1-2](#)
- [ContextAware Tab, page 1-3](#)

Cisco 3300 Series Mobility Services Engines

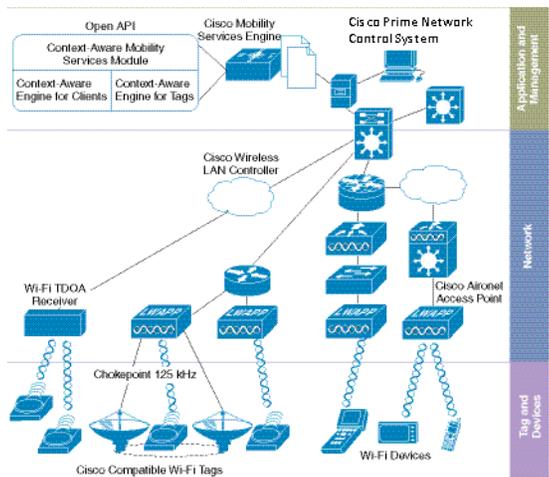
The Cisco 3300 series mobility services engine operates with CAS, which is a component of the CAM solution.

There are three models of the mobility services engine:

- Cisco 3310 Mobility Services Engine
- Cisco 3350 Mobility Services Engine

- Cisco 3355 Mobility Services Engine

Figure 1-1 Context-Aware Mobility Solution



CAS

CAS allows a mobility services engine to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location, temperature, and availability from Cisco access points.

CAS relies on two engines for processing the contextual information it receives. The *Context-Aware Engine for Clients* processes data received from Wi-Fi clients and the *Context-Aware Engine for Tags* processes data received from Wi-Fi tags; these engines can be deployed together or separately depending on the business need.

Licensing Information for Clients and Tags

You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points.

- Licenses for tags and clients are offered separately. (The clients license also includes tracking of rogue clients, rogue access points, interferers, and wired clients.)
- For more information on tags, clients, rogue clients, and rogue access points, see [Chapter 9, “Context-Aware Service Planning and Verification”](#)
- Licenses for tags and clients are offered in various quantities, ranging from 1,000 to 12,000 units. Up to 25,000 Wi-Fi clients and Wi-Fi tags (combined count) are supported depending on the mobility services engine hardware.
 - The Cisco 3310 mobility services engine supports up to 2,000 clients and tags (combined count).
 - The Cisco 3355 mobility services engine supports up to 25,000 clients and tags (combined count).

- For details on tag and client licenses, see the *Cisco 3300 Series Mobility Services Engine Release Note, Release 6.0* at the following URL:
http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

Guidelines and Limitations

Username, IP address, and partial MAC address-based troubleshooting is supported only on MSE Release 7.0.200.0 and later.

Viewing Contextual Information

The collected contextual information can be viewed in graphical user interface format in the Prime Infrastructure on the centralized WLAN management platform.



Note

However, before you can use Prime Infrastructure, initial configuration for the mobility services engine is required using a command-line interface console session. See the *Cisco 3350 Mobility Services Engine Getting Started Guide* and the *Cisco 3100 Mobility Services Engine Getting Started Guide* at the following URL:

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

After its installation and initial configuration are complete, the mobility services engine can communicate with multiple Cisco wireless LAN controllers to collect operator-defined contextual information. You can then use the associated Prime Infrastructure to communicate with each mobility services engine to transfer and display selected data.

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

This section contains the following topics:

- [ContextAware Tab, page 1-3](#)
- [Location Assisted Client Troubleshooting from the ContextAware Dashboard, page 1-4](#)

ContextAware Tab

You can access the ContextAware tab in the Prime Infrastructure home page. This tab provides you with important Context-Aware Service software information.

The following factory default components appear on the ContextAware tab:

- MSE Historical Element Count—Shows the historical trend of tags, clients, rogue APs, rogue clients, interferers, wired clients, and guest client counts in a given period of time.



Note

The MSE Historical Element Count information is presented in a time-based graph. For graphs that are time-based, the top of the graph page includes a link bar that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed.



Note The MSE historical element count for the dashlets are obtained from MSE every 5 minutes and is aggregated in the Prime Infrastructure database at regular intervals. For a given virtual domain, element counts are obtained from the MSE based on floors assigned to that virtual domain. These counts are aggregated and displayed in the dashlet.

- Rogue Element Detected by CAS—Shows the indices of the Rogue APs and Rogue Clients in percentage. It also provides a count of the number of Rogue APs and Rogue Clients detected by each MSE within an hour, 24 hours, and more than 24 hours.

Rogue AP Index is defined as the percentage of total active tracked elements that are detected as Rogue APs across all the MSEs on the Prime Infrastructure.

Rogue Client Index is defined as the percentage of total active tracked elements that are detected as Rogue Clients across all the MSEs on the Prime Infrastructure.

- Location Assisted Client Troubleshooting—You can troubleshoot clients using this option with location assistance. You can provide a MAC address, username, or IP address as the criteria for troubleshooting.



Note Username, IP address, and partial MAC address-based troubleshooting are supported only on MSE Release 7.0.200.0 and later.

For more information about Location Assisted Client Troubleshooting, see the [“Location Assisted Client Troubleshooting from the ContextAware Dashboard”](#) section on page 1-4.

- MSE Tracking Counts—Represents the tracked and non-tracked count of each of the element types. The element type includes tags, rogue APs, rogue clients, interferers, wired clients, wireless clients, and guest clients.



Note The non-tracked element count is available only in root domain.

- Top 5 MSEs—Lists the top five MSEs based on the percentage of license utilization. It also provides the count for each element type for each MSE.
- In the component, click the count link to get a detailed report.
- Use the icons in a component to switch between chart and grid view.
- Use the Enlarge Chart icon to view the grid or chart in full page.

Location Assisted Client Troubleshooting from the ContextAware Dashboard

You can use the ContextAware tab in the Prime Infrastructure home page to troubleshoot a client. Specify a MAC address, username, or IP address as the search criteria, and click **Troubleshoot**. The Troubleshoot page appears. Through the dashboard, troubleshooting information is displayed for

wireless clients that belong to a given virtual domain. In case of the associated clients, troubleshooting information is displayed only if it belongs to a floor in the given virtual domain. In case of probing clients, troubleshooting information is displayed in the root domain.

You can view the Context Aware History report on the Context Aware History tab. You can filter this report based on the MSE name. You can further filter the report based on the Timezone, State, or All. The states can be either associated or dissociated.

If you choose Timezone then you can choose any of the following:

- Date and Time

or

- Any one of these values from the drop-down list:
 - Last 1 Hour
 - Last 6 Hours
 - Last 1 Day
 - Last 2 Days
 - Last 3 Days
 - Last 4 Days
 - Last 5 Days
 - Last 6 Days
 - Last 7 Days
 - Last 2 Weeks
 - Last 4 Weeks

Alternately, you can use the Generate Report link to generate a Client Location History report. You can also opt to export the report to CSV or PDF format, or you can e-mail the report using the icons available in the report page.

For more information on the Prime Infrastructure home page ContextAware tab, see the [“ContextAware Tab” section on page 1-3](#).

Event Notification

A mobility services engine sends event notifications to registered listeners over the following transport mechanisms:

- Simple Object Access Protocol (SOAP)
- Simple Mail Transfer Protocol (SMTP) mail
- Simple Network Management Protocol (SNMP)
- Syslog



Note

The Prime Infrastructure can act as a listener receiving event notifications over SNMP. Without event notification, the Prime Infrastructure and third-party applications need to periodically request location information from location-based services.

The pull communication model, however, is not suitable for applications that require more real-time updates to location information. For these applications, you can configure the mobility services engine push event notifications when certain conditions are met by the registered listeners.

Configuration and Administration

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

This section contains the following topics:

- [Adding and Deleting a Mobility Services Engine, page 1-6](#)
- [Synchronizing Mobility Services Engines, page 1-6](#)
- [Configuring High Availability, page 1-6](#)
- [Configuring the Virtual Appliance, page 1-7](#)
- [Editing Mobility Services Engine Properties, page 1-7](#)
- [Managing Users and Groups, page 1-7](#)
- [Synchronizing Mobility Services Engines, page 1-6](#)
- [Monitoring Capability, page 1-8](#)
- [Provisioning MSAP Requirements, page 1-8](#)
- [Maintenance Operations, page 1-8](#)
- [MSE System and Appliance Hardening, page 1-8](#)

Adding and Deleting a Mobility Services Engine

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

Synchronizing Mobility Services Engines

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

Configuring High Availability

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

Configuring the Virtual Appliance

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

Editing Mobility Services Engine Properties

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

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

Managing Users and Groups

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

Configuring Event Notifications

You can use the Prime Infrastructure to define conditions that cause the mobility services engine to send notifications to specific listeners. This chapter describes how to define events and event groups and how to view event notification summaries. See [Chapter 8, “Configuring Event Notifications,”](#) for configuration event notifications.

Context-Aware Planning and Verification

To plan and optimize access point deployment, you can use the Prime Infrastructure to perform point or line calibration. Additionally, you can analyze the location accuracy of non-rogue clients, asset tags and interferers using the accuracy tool. See [Chapter 9, “Context-Aware Service Planning and Verification,”](#) for specifics.

Working with Maps

Maps provide a summary view of all your managed systems on campuses, buildings, outdoor areas, and floors. See [Chapter 10, “Working with Maps,”](#) for more information.

Monitoring Capability

You can use the Prime Infrastructure to monitor alarms, events, and logs generated by mobility services engine. You can also monitor the status of mobility services engines, clients, interferers, and tagged assets. Additionally, you can generate a utilization report for the mobility services engine to determine CPU and memory utilization as well as counts for clients, tags and rogue access points and clients. See [Chapter 11, “Monitoring the System and Services,”](#) for more information.

Provisioning MSAP Requirements

Cisco Mobility Services Advertisement Protocol (MSAP) provides requirements for MSAP client and server and describes the message exchanges between them. Mobile devices can retrieve service advertisements from MSAP server over Wi-Fi infrastructure using MSAP. MSAP is introduced in this release in the mobility services engine (MSE) and provides server functionality. See [Chapter 12, “MSAP,”](#) for more information.

Maintenance Operations

You can back up mobility services engine data to a predefined FTP folder on the Prime Infrastructure at defined intervals, and restore the mobility services engine data from that Prime Infrastructure. Other mobility services engine maintenance operations that you can perform include downloading new software images to all associated mobility services engines from any Prime Infrastructure station, and clearing mobility services engine configurations. See [Chapter 13, “Performing Maintenance Operations,”](#) for more information.

**Note**

Details on recovering GRUB and root passwords for the mobility services engine using the command-line interface (rather than the Prime Infrastructure) are also addressed in [Chapter 13, “Performing Maintenance Operations”](#).

MSE System and Appliance Hardening

System and Appliance Hardening requires some services and processes to be exposed to function properly. Hardening of MSE involves disabling unnecessary services, upgrading to the latest server versions, and applying appropriate restrictive permissions to files, services, and endpoints. See [Appendix A, “MSE System and Appliance Hardening Guidelines”](#) for more information.

System Compatibility

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



CHAPTER 2

Adding and Deleting Mobility Services Engines and Licenses

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



Note

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

This chapter contains the following sections:

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

Licensing Requirements for MSE

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

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

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

This section contains the following topics:

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

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

MSE License Structure Matrix

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

Table 2-1 MSE License Structure Matrix

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

Sample MSE License File

The following is a sample MSE license file:

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

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

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

Revoking and Reusing an MSE License

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

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

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

For more information on licensing, see the *Cisco Prime Infrastructure Configuration Guide, Release 7.3*.

Revoking an MSE License Using the MSE CLI

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

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

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

Guidelines and Limitations

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

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

Adding a Mobility Services Engine to the Prime Infrastructure

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



Tip

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



Note

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

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



Note

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

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

This refers to the Prime Infrastructure communication username and password created during the setup process.

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

The default username and password are both *admin*.



Note

If you changed the username and password during the automatic installation script, enter those values here. If you did not change the default passwords, we recommend that you rerun the automatic installation script and change the username and password.

- Step 8** Select the **HTTP** check box to allow communication between the mobility services engine and third-party applications. By default, the Prime Infrastructure uses HTTPs to communicate with MSE.
- Step 9** Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the mobility services engine.

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

Step 10 Click **Next**. The Prime Infrastructure automatically synchronizes the selected elements with the MSE.

After the synchronization, the MSE License Summary page appears. You can use the MSE License Summary page to install a license, add a license, remove a license, install an activation license, and install service license. The Select Mobility Service page appears.

Step 11 To enable a service on the mobility services engine, select the check box next to the service. Services include Context-Aware Service and wIPS.

You can choose CAS to track clients, rogues, interferers, wired clients, and tags.

Choose either of the following engines to track tags:

- Cisco Tag Engine
- or
- Partner Tag Engine

Step 12 Click **Save**.



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



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

Enabling Services on the Mobility Services Engine

To enable services on the mobility services engine, follow these steps:

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

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

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



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

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



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

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

Configuring MSE Tracking and History Parameters

Step 1 After you enable services on the mobility services engine, the Select Tracking & History Parameters page appears.



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

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

- Wired Clients
- Wireless Clients
- Rogue Access Points
 - Exclude Adhoc Rogue APs
- Rogue Clients
- Interferers
- Active RFID Tags

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

- Wired Stations
- Client Stations
- Rogue Access Points
- Rogue Clients
- Interferers
- Asset Tags

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

Assigning Maps to the MSE



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

- Step 1** Once you configure MSE tracking and history parameters, the Assigning Maps page appears. The Assign Maps page shows the following information:
- Map Name
 - Type (building, floor, campus)
 - Status
- Step 2** You can see the required map type by selecting All, Campus, Building, Floor Area, or Outdoor Area from the Filter option available on the page.
- Step 3** To synchronize a map, select the **Name** check box and click **Synchronize**. Upon synchronization of the network designs, the appropriate controllers that have APs assigned on a particular network design are synchronized with the MSE automatically. Click **Done** to save the MSE settings.

Deleting an MSE License File

To delete an MSE license file, follow these steps:

- Step 1** Choose **Services > Mobility Service Engine**. The Mobility Services page appears.
- Step 2** Click **Device Name** to delete a license file for a particular service.
- Step 3** From the Select a command drop-down list, choose **Edit Configuration**. The Edit Mobility Services Engine dialog box appears.
- Step 4** Click **Next** in the Edit Mobility Services Engine dialog box. The MSE License Summary page appears.
- Step 5** Choose the MSE license file that you want to delete in the MSE License Summary page.
- Step 6** Click **Remove License**.
- Step 7** Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the license.
- Step 8** Click **Next** to enable services on the mobility services engine.

Deleting a Mobility Services Engine from the Prime Infrastructure

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

**Note**

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

-
- Step 1** Choose **Services > Mobility Services**.
The Mobility Services page appears.
- Step 2** Select the mobility services engine to be deleted by selecting the corresponding **Device Name** check box(es).
- Step 3** From the Select a command drop-down list, choose **Delete Service(s)**. Click **Go**.
- Step 4** Click **OK** to confirm that you want to delete the selected mobility services engine from the Prime Infrastructure database.
- Step 5** Click **Cancel** to stop deletion.
-

Registering Device and wIPS Product Authorization Keys

You receive a Product Authorization Key (PAK) when you order a CAS element, wIPS, or tag license from Cisco. You must register the PAK to receive the license file for installation on the mobility services engine. License files are e-mailed to you after successfully registering a PAK.

Client and wIPS PAKs are registered with Cisco.

**Note**

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

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

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

Figure 2-1 Enter PAK Number Page

Worldwide [change] Logged In | Account | About Cisco

Search Go

Solutions Products & Services Ordering Support Training & Events Partner Central

HOME Support

Product License Registration

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

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):*

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

Go Back SUBMIT

276054

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



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

Figure 2-2 Validate Features Page

Worldwide [change] Logged In | Account | About Cisco

Search Go

Solutions Products & Services Ordering Support Training & Events Partner Central

HOME 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.

Go Back Continue

276055

Figure 2-3 Designate Licensee, Page 1 of 2

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



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

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

Figure 2-4 Designate Licensee, Page 2 of 2

Modify the information as necessary.

- Step 6** If the registrant and end user are not the same person, select the **Licensee (End-User)** check box beneath registrant information and enter the information for the end user.
- Step 7** Click **Continue**. A summary of entered data appears (see [Figure 2-5](#)).

Figure 2-5 *Finish and Submit Page*

HOME
Product License Registration

Support
Product License Registration

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

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

Licensee Information

Registrant Profile
[Edit Details](#)

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

End User Profile
[Edit Details](#)

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

Toolkit: Roll over tools below
Feedback | Help

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

276059

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

Figure 2-6 *Registration Confirmation Page*

Worldwide [change] Logged In | Account | About Cisco

Search Go

Solutions Products & Services Ordering Support Training & Events Partner Central

HOME
Product License Registration

Support
Product License Registration

Registration Complete

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

Toolkit: Roll over tools below
Feedback | Help

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

276060

Installing Device and wIPS License Files

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



Note

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



Note

The **Administration > License Center** page is available only in the virtual domain in Release 7.3.

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

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

-
- Step 1** Choose **Administration > License Center**.
 - Step 2** Choose **Files > MSE Files** from the left sidebar menu.
 - Step 3** Click **Add**. The Add a License File dialog box appears.
 - Step 4** Choose the applicable MSE name from the MSE Name drop-down list.



Note

Verify that the UDI of the selected mobility services engine matches the one you entered when registering the PAK.

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

Registering Tag PAKs

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

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

Installing Tag Licenses

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

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



CHAPTER 3

Synchronizing Mobility Services Engines

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



Note

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

This chapter contains the following sections:

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

Information About Synchronizing the Prime Infrastructure and Mobility Services Engines

This section describes how to synchronize the Prime Infrastructure and mobility services engines manually and automatically.



Note

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

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

- **Network Design**—A logical mapping of the physical placement of access points throughout facilities. A hierarchy of a single campus, the buildings that comprise that campus, and the floors of each building constitute a single network design.
- **Controller**—A selected controller that is associated and regularly exchanges location information with a mobility services engine. Regular synchronization ensures location accuracy.
- **Wired Switches**—Wired Catalyst switches that provide an interface to wired clients on the network. Regular synchronization ensures that location tracking of wired clients in the network is accurate.

- The mobility services engine can be synchronized with Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports.
- The mobility services engine can also be synchronized with the following Catalyst 4000 series switches: WS-C4948, WS-C4948-10GE, ME-4924-10GE, WS-4928-10GE, WS-C4900M, WS-X4515, WS-X4516, WS-X4013+, WS-X4013+TS, WS-X4516-10GE, WS-X4013+10GE, WS-X45-SUP6-E, and WS-X45-SUP6-LE.
- Event Groups—A group of predefined events that define triggers that generate an event. Regular synchronization ensures that the latest defined events are tracked. Event groups can also be created by third-party applications. For more information on third-party application created event groups, see the “[Configuring Automatic Database Synchronization and Out-of-Sync Alerts](#)” section on page 3-5.
- Third Party Elements—When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.
- Service Advertisements—MSAP provides service advertisements on mobile devices. This shows the service advertisement that is synchronized with the MSE.

Prerequisites for Synchronizing the Mobility Services Engine

- Be sure to verify software compatibility between the controller, Prime Infrastructure, and the mobility services engine before synchronizing. See the latest mobility services engine release notes at the following URL:
http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html
- Communication between the mobility services engine, Prime Infrastructure, and the controller is in Coordinated Universal Time (UTC). Configuring NTP on each system provides devices with UTC time. The mobility services engine and its associated controllers must be mapped to the same NTP server and the same Prime Infrastructure server. An NTP server is required to automatically synchronize time between the controller, Prime Infrastructure, and the mobility services engine. However, the timezone for MSE should still be set to UTC. This is because wIPS alarms require that the MSE time be set to UTC.

Working with Third-Party Elements

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

Deleting Elements or Marking Them as Third-Party Elements

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

-
- Step 1** Choose **Services > Synchronize Services**.
The Network Designs page appears.
 - Step 2** In the Network Designs page, choose **Third Party Elements** from the left sidebar menu.

The Third Party Elements page appears.

Step 3 Select one or more elements.

Step 4 Click one of the following buttons:

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

Synchronizing Controllers with a Mobility Services Engine

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

Synchronizing a Controller, Catalyst Switch, or Event Group

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

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

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

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

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

The Network Designs page appears.

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



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

Step 5 Click **Change MSE Assignment**.

Step 6 Select the mobility services engine to which the maps are to be synchronized.

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

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

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



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



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

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

Assigning an MSE to the Controller

To assign a mobility services engine with any wireless controller on a per-service basis (CAS or WIPS), follow these steps:

- Step 1** Choose **Services > Synchronize Services**.
- Step 2** In the Network Designs page, choose **Controller** from the left sidebar menu.
- Step 3** Select the controllers to be assigned to the mobility services engine by selecting the corresponding **Name** check box.
- Step 4** Click **Change MSE Assignment**.
- Step 5** Choose the mobility services engine to which the controllers must be synchronized.
- Step 6** Click either of the following in the Choose MSEs dialog box:
- **Save**—Saves the mobility services engine assignment. The following message appears in the Messages column of the Controllers page with a yellow arrow icon:
“To be assigned - Please synchronize.”
 - **Cancel**—Discards the changes to mobility services engine assignment and returns to the Controllers page.
- You can also click **Reset** to undo the mobility services engine assignments.
- Step 7** Click **Synchronize** to complete the synchronization process.
- Step 8** Verify that the mobility services engine is communicating with each of the controllers for only the chosen service. This can be done by clicking the NMSP status link in the status page.



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

**Note**

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

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

**Note**

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

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

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

- Step 1** Choose **Services > Synchronize Services**.
- Step 2** From the left sidebar menu, choose the appropriate menu options.
- Step 3** Select one or more elements by selecting the **Name** check box, and click **Change MSE Assignment**. The Choose MSEs dialog box appears.
- Step 4** Unselect the mobility services engine if you do not want the elements to be associated with that mobility services engine by selecting either the **CAS** or **wIPS** check box.
- Step 5** Click **Save** to save the assignment changes.
- Step 6** Click **Synchronize**.
The Sync Status column appears blank.

Configuring Automatic Database Synchronization and Out-of-Sync Alerts

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

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

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

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

This section contains the following topics:

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

Configuring Automatic Database Synchronization

To configure smart synchronization, follow these steps:

-
- Step 1** Choose **Administration > Background Tasks**.
- Step 2** Select the **Mobility Service Synchronization** check box.
The Mobility Services Synchronization page appears.
- Step 3** To set the mobility services engine to send out-of-sync alerts, select the Out of Sync Alerts **Enabled** check box.
- Step 4** To enable smart synchronization, select the Smart Synchronization **Enabled** check box.



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



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

- Step 5** Enter the time interval, in minutes, that the smart synchronization is to be performed.
By default, the smart-sync is enabled.
- Step 6** Click **Submit**.
-

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

Smart Controller Assignment and Selection Scenarios

Scenario 1

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

Scenario 2

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

Scenario 3

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

Scenario 4

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

Out-of-Sync Alarms

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

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

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

- The mobility services engine is deleted



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

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

Viewing Mobility Services Engine Synchronization Status

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

This section contains the following topics:

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

Viewing Mobility Services Engine Synchronization Status

To view the synchronization status, follow these steps:

-
- Step 1** Choose **Services > Synchronize Services**.
- Step 2** From the left sidebar menu, choose **Network Designs, Controllers, Event Groups, Wired Switches, Third Party Elements, or Service Advertisements**.

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

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

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

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

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

Viewing Synchronization History

You can view the synchronization history for the last 30 days for a mobility services engine. This is especially useful when automatic synchronization is enabled as alarms are automatically cleared. Synchronization history provides a summary of those cleared alarms.

To view synchronization history choose **Services > Synchronization History**. The Synchronization History page appears.

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

Table 3-1 Synchronization History Page

Text Boxes	Description
Timestamp	The date and time at which the synchronization has happened.
Server	The mobility services engine server.
Element Name	The name of element that was synchronized.
Type	The type of the element that was synchronized.
Sync Operation	The sync operation that was performed. It can be an Update, Add, or Delete.
Generated By	The method of synchronization. It can be Manual or Automatic.

Table 3-1 Synchronization History Page

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

Click the column headings to sort the entries.



CHAPTER 4

Configuring High Availability

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

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



Note

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

This chapter contains the following sections:

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

Overview to the High Availability Architecture

This section provides an overview of the high availability architecture:

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

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

Pairing Matrix

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

Table 4-1 Pairing Matrix

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

Guidelines and Limitations for High Availability

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

Failover Scenario for High Availability

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

**Note**

One secondary MSE can back up multiple primary MSEs.

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

Failback

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

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

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

HA Licensing

For HA, activation license is required on the primary and secondary Virtual Appliance. CAS or wIPS license is not required on the secondary MSE. It is only required on the primary MSE.

Configuring High Availability on the MSE

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

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

**Note**

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



Note By default, all MSEs are configured as primary.



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

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

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

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

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

- Step 5** Configure the hostname:

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

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

- Step 6** Configure the domain name:

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

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

- Step 7** Configure the HA role:

```
Current role=[Primary]
Configure High Availability? (Y)es/(S)kip/(U)se default [Skip]:
```

```
High availability role for this MSE (Primary/Secondary):
```

```
Select role [1 for Primary, 2 for Secondary] [1]: 1
```

```
Health monitor interface holds physical IP address of this MSE server.
```

```
This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to
communicate among themselves
```

```
Select Health Monitor Interface [eth0/eth1] [eth0]:eth0
```

```

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

```

Step 8 Configure Ethernet interface parameters:

```

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

```

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

```

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

```

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

Step 10 Configure the hostname for the secondary MSE:

```

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

```

Step 11 Configure the domain name:

```

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

```

Step 12 Configure the HA role:

```

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

```

Step 13 Configure Ethernet interface parameters:

```

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

```

```

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

```

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

Viewing Configured Parameters for High Availability

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

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

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

Viewing High Availability Status

To view the high availability status, follow these steps:

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



CHAPTER 5

MSE Delivery Modes

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

This chapter contains the following sections:

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

Physical Appliance

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



Note

Virtual appliance licenses are not allowed on physical appliances.

Virtual Appliance

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



Note

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

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

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

**Note**

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

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

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

This section contains the following topics:

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

Operating Systems Requirements

The following operating systems are supported:

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

**Note**

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

Client Requirements

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

**Note**

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

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

Prerequisites for Setting Up an MSE Virtual Appliance on a Server

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

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

Virtual Appliance Sizing

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

Table 5-1 Virtual Appliance Sizing

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

Reinstalling the MSE on a Physical Appliance

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

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

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

Deploying the MSE Virtual Appliance

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

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

Deploying the MSE Virtual Appliance from the VMware vSphere Client

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



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

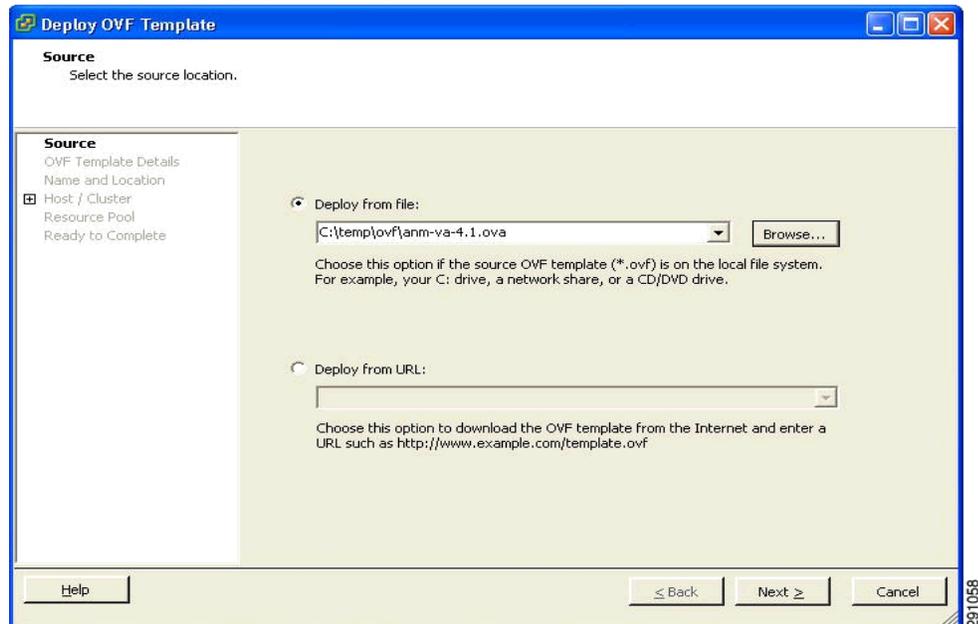


Note Deploying virtual appliance takes at least 500 GB of available disk space on the ESXi host database. We recommend that the datastore on the host have a block size of at least 4 MB or more for ESXi 4.1 or earlier, else the deployment may fail. No such restriction is placed on the datastores on ESXi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

To deploy the MSE virtual appliance, follow these steps:

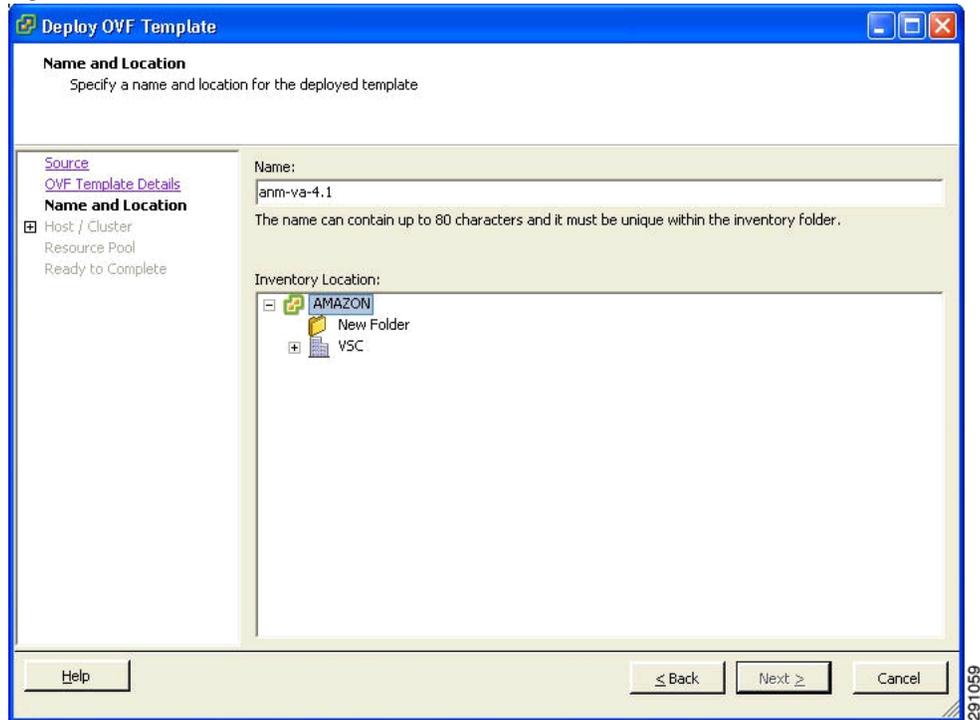
- Step 1** From the VMware vSphere Client main menu, choose **File > Deploy OVF Template**. The OVF Template Source window appears (see [Figure 5-1](#)).

Figure 5-1 Deploy OVF Template Window



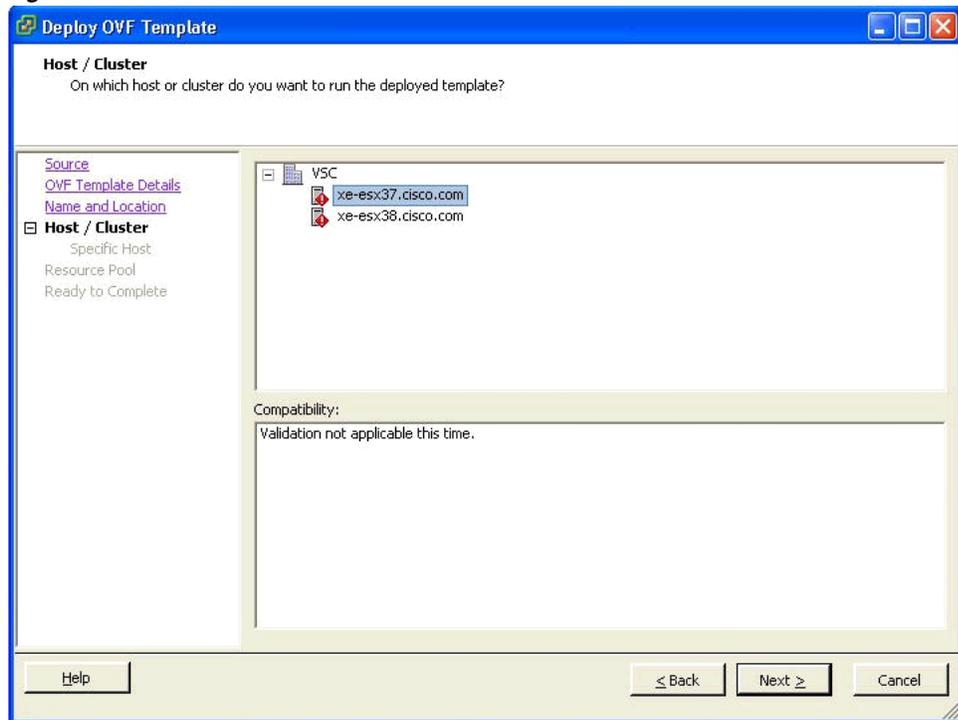
- Step 2** Select the **Deploy From File** radio button and choose the OVA file that contains the MSE virtual appliance distribution from the drop-down list.
- Step 3** Click **Next**. The OVF Template Details window appears. VMware ESX/ESXi reads the OVA attributes. The details include the product you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

Figure 5-2 Name and Location Window



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

Figure 5-3 Host/Cluster Window



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

Configuring the Basic Settings to Start the MSE Virtual Appliance VM

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

To start the MSE setup, follow these steps:

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

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

Deploying the MSE Virtual Appliance Using the Command-Line Client

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

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

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

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

Adding a Virtual Appliance License to the Prime Infrastructure

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

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

Adding a License File to the MSE Using the License Center

To add a license, follow these steps:

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

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

Viewing the MSE License Information Using the License Center

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

- Step 1** Choose **Administration > License Center** to access the License Center page.
- Step 2** Choose **Summary > MSE** from the left sidebar menu to view the MSE summary page.
[Table 5-2](#) lists the MSE Summary page fields.

Table 5-2 MSE Summary Page

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

Removing a License File Using the License Center

To remove a license, follow these steps:

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

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



CHAPTER 6

Configuring and Viewing System Properties

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

This chapter contains the following sections:

- [Licensing Requirement, page 6-1](#)
- [Editing General Properties and Viewing Performance, page 6-1](#)
- [Viewing Active Sessions on a System, page 6-4](#)
- [Adding and Deleting Trap Destinations, page 6-5](#)
- [Viewing and Configuring Advanced Parameters, page 6-7](#)
- [Initiating Advanced Parameters, page 6-7](#)

Licensing Requirement

All mobility services engines are shipped with an evaluation license of CAS and wIPS. Evaluation copies are good for a period of 60 days (480 hours) and have preset device limits for each service. Licenses are usage-based (time is decremented by the number of days you use it rather than by the number of calendar days passed).

When you are applying an evaluation license to MSE, the behavior is slightly different from a permanent license. Firstly, an evaluation license for MSE will only increase the evaluation period but not the count of the licensed elements. Secondly, when an evaluation license is applied, there is no license file copied to MSE. Instead the update is made directly in the MSE database. Also, you will not see the license information under License Center > Files > MSE page.

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

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

Editing General Properties and Viewing Performance

General Properties—You can use the Cisco Prime Infrastructure to edit the general properties of a mobility services engine such as contact name, username, password, services enabled on the system, enabling or disabling a service, or enabling the mobility services engine for synchronization. See the [“Editing General Properties” section on page 6-2](#) for more information.

**Note**

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

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

This section contains the following topics:

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

Editing General Properties

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

- Step 1** Choose **Services > Mobility Services Engines** to display the Mobility Services page.
- Step 2** Click the name of the mobility services engine you want to edit. Two tabs appear with the following headings: General and Performance.

**Note**

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

- Step 3** Modify the fields as appropriate on the General tab. [Table 6-1](#) lists the General Properties page fields.

Table 6-1 **General Tab**

Field	Configuration Options
Device Name	User-assigned name for the mobility services engine.
Device Type	Indicates the type of mobility services engine (for example, Cisco 3310 Mobility Services Engine). Indicates whether the device is a virtual appliance or not.
Device UDI	The Device UDI (Unique Device Identifier) is the string between double quote characters (including spaces in the end if any).
Version	Version of product identifier.
Start Time	Indicates the start time when the server was started.
IP Address	Indicates the IP address for the mobility services engine.
Contact Name	Enter a contact name for the mobility services engine.
Username	Enter the login username for the Prime Infrastructure server that manages the mobility services engine. This replaces any previously defined username including any set during initial setup.
Password	Enter the login password for the Prime Infrastructure server that manages the mobility services engine. This replaces any previously defined password including any set during initial setup.

Table 6-1 General Tab (continued)

Field	Configuration Options
HTTP	<p>Select the Enable check box to enable HTTP. By default, HTTPS is enabled.</p> <p>Note HTTP is primarily enabled to allow third-party applications to communicate with the mobility services engine.</p> <p>Note Prime Infrastructure always communicates through HTTPS.</p>
Legacy Port	Enter the mobility services port number that supports HTTPS communication. The Legacy HTTPS option must also be enabled.
Legacy HTTPS	This does not apply to mobility services engines. It applies only to location appliances.
Delete synchronized service assignments and enable synchronization	Select this check box if you want to permanently remove all service assignments from the mobility services engine. This option is available only if the delete synchronized service assignments check box was unselected while adding a mobility services engine.
Mobility Services	<p>To enable a service on the mobility services engine, select the check box next to the service. The services include Context Aware and wIPS.</p> <p>You can choose CAS to track clients, rogues, interferers, wired clients, and tags.</p> <p>Choose either of the following engines to track tags:</p> <ul style="list-style-type: none"> • Cisco Tag Engine <li style="padding-left: 20px;">or • Partner Tag Engine <p>Note Once selected, the service is displayed as Up (active). All inactive services are noted as Down (inactive) on the selected (current) system and on the network.</p> <p>Note CAS and wIPS can operate on a mobility services engine at the same time.</p> <p>Click the here link to see the number of devices that can be assigned for the current system.</p> <p>In the License Center page, choose MSE from the left sidebar menu option to see the license details for all mobility services engines on the network.</p> <p>Note For more information on purchasing and installing licenses, see the following URL:</p> <p>http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html</p>

**Note**

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

**Note**

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

**Note**

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

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

Viewing Performance Information

To view performance details, follow these steps:

-
- Step 1** Choose **Services > Mobility Services** to display the Mobility Services page.
- Step 2** Click the name of the mobility services engine you want to view. Two tabs appear with the following headings: General and Performance.
- Step 3** Click the **Performance** tab.
- Click a time period (such as *1w*) on the y-axis to see performance numbers for periods greater than one day.
- To view a textual summary of performance, click the second icon under CPU.
- To enlarge the page, click the icon at the lower right.
-

Viewing Active Sessions on a System

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

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

- Session identifier
- IP address from which the mobility services engine is accessed
- Username of the connected user
- Date and time when the session started

- Date and time when the mobility services engine was last accessed
- How long the session was idle since it was last accessed

To view active user sessions, follow these steps:

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

Adding and Deleting Trap Destinations

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

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

This section contains the following topics:

- [Adding Trap Destinations, page 6-5](#)
- [Deleting Trap Destinations, page 6-6](#)

Adding Trap Destinations

To add a trap destination, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the mobility services engine for which you want to define a new SNMP trap destination server.
- Step 3** Choose **System > Trap Destinations**.
- Step 4** From the Select a command drop-down list, choose **Add Trap Destination**. Click **Go**.

The New Trap Destination page appears.

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

Table 6-2 Add Trap Destination Page Fields

Field	Description
IP Address	IP address for the trap destination.
Port No.	Port number for the trap destination. The default port number is 162.

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

Field	Description
Destination Type	This field is not editable and has a value of Other.
SNMP Version	Choose either v2c or v3 from the SNMP Version drop-down list.
The following set of fields appear only if you select v3 as the SNMP version.	
User Name	Username for the SNMP Version 3.
Security Name	Security name for the SNMP Version 3.
Auth. Type	Choose either of the following from the drop-down list: <ul style="list-style-type: none"> • HMAC-MD5 • HMAC-SHA
Auth. Password	Authentication password for the SNMP Version 3.
Privacy Type	Choose one of the following from the drop-down list: <ul style="list-style-type: none"> • CBC-DES • CFB-AES-128 • CFB-AES-192 • CFB-AES-256
Privacy Password	Privacy password for the SNMP Version 3.



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

Step 5 Click **Save**.

You are returned to the Trap Destination Summary page and the newly defined trap is listed.

Deleting Trap Destinations

To delete a trap destination, follow these steps:

- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the mobility services engine for which you want to delete a SNMP trap destination server.
- Step 3** Choose **System > Trap Destinations**.
- Step 4** Select the check box next to the trap destination entry that you want to delete.
- Step 5** From the Select a command drop-down list, choose **Add Trap Destination**. Click **Go**.

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

Viewing and Configuring Advanced Parameters

In the Prime Infrastructure Advanced Parameters page you can view general system level settings of the mobility services engine and configure monitoring parameters.

- See the “[Viewing Advanced Parameter Settings](#)” section on page 6-7 to view current system-level advanced parameters.
- See the “[Initiating Advanced Commands](#)” section on page 6-8 to modify the current system-level advanced parameters or initiate advanced commands such as system reboot, system shut down, or clear a configuration file.

Viewing Advanced Parameter Settings

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

-
- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of a mobility services engine to view its status.
- Step 3** Choose **System > Advanced Parameters**.
-

Initiating Advanced Parameters

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



Note You can use the Prime Infrastructure to modify troubleshooting parameters for a mobility services engine or a location appliance.

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

- To set how long events are kept and amount of time before a session times out.
For more information, see the “[Configuring Advanced Parameters](#)” section on page 6-7.
- To initiate a system reboot or shutdown, or clear the system database.
For more information, see the “[Initiating Advanced Commands](#)” section on page 6-8.

Configuring Advanced Parameters

To configure advanced parameters, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the mobility service whose properties you want to edit.
- Step 3** From the left sidebar menu, choose **System > Advanced Parameters**.
- Step 4** View or modify the advanced parameters as necessary.

- General Information
 - Product Name
 - Version
 - Started At
 - Current Server Time
 - Hardware Restarts
 - Active Sessions
- Advanced Parameters

**Caution**

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

- Number of Days to keep Events—Enter the number of days to keep logs. Change this value as required for monitoring and troubleshooting.
- Session Timeout—Enter the number of minutes before a session times out. Change this value as required for monitoring and troubleshooting. Currently this option appears dimmed.
- Cisco UDI
 - Product Identifier (PID)—The product ID of the mobility services engine.
 - Version Identifier (VID)—The version number of the mobility services engine.
 - Serial Number (SN)—Serial number of the mobility services engine.
- Advanced Commands
 - Reboot Hardware—Click to reboot the mobility services hardware. See the [“Rebooting or Shutting Down a System” section on page 6-9](#) for more information.
 - Shutdown Hardware—Click to turn off the mobility services hardware. See the [“Rebooting or Shutting Down a System” section on page 6-9](#) for more information.
 - Clear Database—Click to clear the mobility services database. See the [“Clearing the System Database” section on page 6-9](#) for more information. Unselect the **Retain current service assignments in Prime Infrastructure** check box to remove all existing service assignments from the Prime Infrastructure and MSE. The resources must be reassigned in the Services > Synchronize Services page. By default, this option is selected.

- Step 5** Click **Save** to update the Prime Infrastructure and mobility services engine databases.
-

Initiating Advanced Commands

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

This section contains the following topics:

- [Rebooting or Shutting Down a System, page 6-9](#)
- [Clearing the System Database, page 6-9](#)

Rebooting or Shutting Down a System

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

-
- Step 1** Choose **Services > Mobility Services Engines**.
 - Step 2** Click the name of a mobility services engine you want to reboot or shut down.
 - Step 3** Choose **System > Advanced Parameters**.
 - Step 4** In the Advanced Commands group box, click the appropriate button (**Reboot Hardware** or **Shutdown Hardware**).

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

Clearing the System Database

To clear a mobility services engine configuration and restore its factory defaults, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**.
 - Step 2** Click the name of the mobility services engine you want to configure.
 - Step 3** Choose **System > Advanced Parameters**.
 - Step 4** In the Advanced Commands group box, unselect the **Retain current service assignments in Prime Infrastructure** check box to remove all existing service assignments from the Prime Infrastructure and MSE.

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

- Step 5** In the Advanced Commands group box, click **Clear Database**.
 - Step 6** Click **OK** to clear the mobility services engine database.
-



CHAPTER 7

Managing Users and Groups

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

This chapter contains the following sections:

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

Prerequisites

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

Guidelines and Limitations

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

Managing User Groups

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

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

This section contains the following topics:

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

Adding User Groups

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



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

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



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

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

Deleting User Groups

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

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

Changing User Group Permissions



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

To change user group permissions, follow these steps:

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

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

Managing Users

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

This section contains the following topics:

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

Adding Users



Caution

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

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

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



Note

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

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

Deleting Users

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

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

Changing User Properties

To change user properties, follow these steps:

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



CHAPTER 8

Configuring Event Notifications

With the Cisco Prime Infrastructure, you can define conditions that cause the mobility services engine to send notifications to specific listeners. This chapter describes how to define events and event groups and how to view event notification summaries.



Note

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

This chapter contains the following sections:

- [Information About Event Notifications, page 8-1](#)
- [Adding and Deleting Event Groups, page 8-7](#)
- [Adding, Deleting, and Testing Event Definitions, page 8-8](#)
- [Viewing Event Notification Summary, page 8-12](#)
- [Clearing Notifications, page 8-2](#)
- [Notification Message Formats, page 8-3](#)
- [The Prime Infrastructure as a Notification Listener, page 8-6](#)

Information About Event Notifications

- **Event Group**—Helps you to organize your event notifications.
- **Event Definition**—An event definition contains the condition that caused the event, the assets to which the event applies, and the event notification destination.
- **Event Notification**—A mobility services engine sends event notifications to registered listeners over the following transport mechanisms.
 - Simple Object Access Protocol (SOAP)
 - Simple Mail Transfer Protocol (SMTP) mail
 - Simple Network Management Protocol (SNMP)
 - Syslog

This section contains the following topics:

- [“Viewing Event Notification Summary” section on page 8-2](#)

- “Clearing Notifications” section on page 8-2
- “Notification Formats in XML” section on page 8-3

Viewing Event Notification Summary

The mobility services engine sends event notifications and does not store them. However, if the Prime Infrastructure is a destination of notification events, it stores the notifications it receives and groups them into the following seven categories:

- **Absence (Missing)**—The mobility services engine generates an absence event when an asset goes missing. In other words, the mobility services engine cannot detect the asset in the WLAN for the specified time.
- **In/Out Area (Containment)**—The mobility services engine generates a containment event when an asset moves in or out of a designated area.



Note You define a containment area (campus, building, or floor) in Monitor > Maps. You can define a coverage area using the Map Editor.

- **Movement from Marker (Movement/Distance)**—The mobility services engine generates a movement event when an asset is moved beyond a specified distance from a designated marker you define on a map.
- **Location Changes**—The mobility services engine generates location change events when a client station, asset tag, rogue client, or rogue access point changes its location.
- **Battery Level**—The mobility services engine generates battery level events for all tracked asset tags.
- **Emergency**—The mobility services engine generates an emergency event for a Cisco CX v.1-compliant asset tag when the panic button of the tag is triggered or the tag becomes detached, is tampered with, becomes inactive, or reports an unknown state. This information is reported and displayed only for Cisco CX v.1-compliant tags.
- **Chokepoint Notifications**—The mobility services engine generates an event when a tag is stimulated by a chokepoint. This information is reported and displayed only for Cisco CX v.1-compliant tags.



Note All element events are summarized hourly and daily.



Note The Track Group and events must be synchronized with a mobility services engine.

Clearing Notifications

A mobility services engine sends event notifications when it clears an event condition in one of the following scenarios:

- **Missing (Absence)**—Elements (clients, tags, rogue access points, or rogue clients) reappear.
- **In/Out Area (Containment)**—Elements move back in to or out of the containment area.
- **Distance**—Elements move back within the specified distance from a marker.
- **Location Changes**—Clear state does not apply to this condition.

- Battery Level—Tags are detected and operate with normal battery level.

**Note**

In the Prime Infrastructure, the Notifications Summary page reflects whether notifications for cleared event conditions have been received.

Notification Message Formats

This section describes the notification message formats for XML and text and contains the following topics:

- [“Notification Message Formats” section on page 8-3](#)
- [“Notification Formats in Text” section on page 8-6](#)

Notification Formats in XML

This section describes the XML format of notification messages and contains the following topics:

- [“Missing \(Absence\) Condition” section on page 8-3](#)
- [“In/Out \(Containment\) Condition” section on page 8-4](#)
- [“Distance Condition” section on page 8-4](#)
- [“Battery Level” section on page 8-5](#)
- [“Location Change” section on page 8-5](#)
- [“Chokepoint Condition” section on page 8-5](#)
- [“Emergency Condition” section on page 8-5](#)

**Note**

The XML format is part of a supported API. Cisco provides change notification as part of the Mobility Services Engine API program whenever the API is updated in the future.

Missing (Absence) Condition

Message format for element absence:

```
<AbsenceTrackEvent
missingFor="<time in secs entity has been missing>"
lastSeen="time last seen"
trackDefn="<name of track definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

Message format for the clear state:

```
<AbsenceTrackEvent
state="clear"
trackDefn="<name of track definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

For example:

```
<AbsenceTrackEvent state="set" missingFor="34" lastSeen="15:00:20 08 Jun 2009"
trackDefn="absenceDef1" entityType="Mobile Station"
entityID="00:0c:f1:53:9e:c0"/>
```

```
<AbsenceTrackEvent state="clear" entityType="Tag"
trackDefn="absenceDef1" entityID="00:0c:cc:5b:fc:da"/>
```

In/Out (Containment) Condition

Message format for element containment:

```
<ContainmentTrackEvent
in="true | false"
trackDefn="<name of track definition>"
containerType="Floor | Area | Network Design | Building"
containerID="<fully qualified name of container>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

Message format for the clear state:

```
<ContainmentTrackEvent
state="clear"
trackDefn="<name of track definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

For example:

```
<ContainmentTrackEvent in="true" trackDefn="myContainerRule1"
containerType="Area"
containerID="nycTestArea,5th Floor,Bldg-A,Rochester_Group,Rochester,"
```



Note The containerID string represents a coverage area called nycTestArea, located in the 5th floor of Bldg-A of the campus Rochester.

```
entityType="Tag" entityID="00:0c:cc:5b:fa:44"/>
```

```
<ContainmentTrackEvent state="clear" entityType="Tag"
trackDefn="myContainerRule1" entityID="00:0c:cc:5b:f8:ab"/>
```

Distance Condition

Message format for elements on the same floor:

```
<MovementTrackEvent
distance="<distance in feet at which the element was located>"
triggerDistance="<the distance specified on the condition>"
reference="<name of the marker specified on the condition>"
trackDefn="<name of event definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

Message format for elements located on a different floor:

```
<MovementTrackEvent optionMsg="has moved beyond original floor"
reference="<name of the marker specified on the condition>"
trackDefn="<name of event definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

Message format for clear state:

```
<MovementTrackEvent
state="clear"
trackDefn="<name of event definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

For example:

```
<MovementTrackEvent distance="115.73819627990147" triggerDistance="60.0"
reference="marker2" trackDefn="distance2" entityType="Mobile Station"
entityID="00:0c:41:15:99:92"/>
```

```
<MovementTrackEvent optionMsg="has moved beyond original floor"
reference="marker2" entityType="Tag"
trackDefn="distance2"
entityID="00:0c:cc:5b:fa:4c"/>
```

```
<MovementTrackEvent state="clear" entityType="Tag"
```

Battery Level

Example:

```
<BatteryLifeTrackEvent lastSeen="10:28:52 08 Jun 2009" batteryStatus="medium"
trackDefn="defn1" entityType="Tag" entityID="00:01:02:03:04:06"/>
```

Location Change

Example:

```
<MovementTrackEvent distance="158.11388300841898" triggerDistance="5.0"
reference="marker1" referenceObjectID="1" trackDefn="defn1" entityType="Mobile Station"
entityID="00:01:02:03:04:05"/>
```

Chokepoint Condition

Example:

```
<ChokepointTrackEvent
lastSeen="11:10:08 PST 08 Jun 2009"
chokepointMac="00:0c:cc:60:13:a3"
chokepointName="chokeA3"
trackDefn="choke"
entityType="Tag"
entityID="00:12:b8:00:20:4f"/>
```

An example for the clear state follows:

```
<ChokepointTrackEvent
state="clear"
entityType="Tag"
trackDefn="choke"
entityID="00:12:b8:00:20:4f"/>
```

Emergency Condition

An example for element location follows:

```
<ChokepointTrackEvent
lastSeen="11:36:46 PST June 08 2009"
emergencyReason= "detached"
trackDefn="emer"
entityType="Tag"
entityID="00:12:b8:00:20:50"/>
```

**Note**

Emergency events are never cleared.

Notification Formats in Text

When you specify that notification be sent in text format, the mobility services engine uses a plain-text string to indicate the condition:

```
Tag 00:02:02:03:03:04 is in Floor <floorName>
Tag 00:02:02:03:03:04 is outside Floor <floorName>
Client 00:02:02:03:09:09 is in Area <areaName>
RogueClient 00:02:02:08:08:08 is outside Building <buildingName>
Tag 00:02:02:03:03:06 has moved 105 feet where the trigger distance was 90 feet.
Tag 00:02:02:03:03:20 missing for 14 mins, last seen <timestamp>.
```

**Note**

Cisco maintains the right to modify the text notification format without notice.

**Note**

XML is the recommended format for systems that need to parse or analyze notification contents.

The Prime Infrastructure as a Notification Listener

The Prime Infrastructure acts as a notification listener.

The Prime Infrastructure translates the traps into user interface alerts and shows them in the following formats:

- Missing (Absence)

Absence of Tag with MAC 00:0c:cc:5b:e4:1b, last seen at 16:19:45 08 June 2009.

- In/Out (Containment)

Tag with MAC 00:0c:cc:5b:fa:44 is In the Area 'Rochester > Rochester > 5th Floor > nycTestArea'

- Distance

Tag with MAC 00:0c:cc:5b:fa:47 has moved beyond the distance configured for the marker 'marker2'.

Tag with MAC 00:0c:cc:5b:f9:b9 has moved beyond 46.0 ft. of marker 'marker2', located at a range of 136.74526528595058 ft.

- Battery Level

Tag 00:01:02:03:04:06 has medium battery, last seen 11:06:01 08 June 2009

- Location Change

Mobile Station 00:01:02:03:04:05 has moved

158.11388300841898ft, where the trigger distance was 5.0

Guidelines and Limitations

If the MAC address that you are using while adding an event definition is a partial MAC address, then it might cause a performance issue in the Prime Infrastructure.

Adding and Deleting Event Groups

This section describes how to add and delete event groups. Event groups help you organize your event notifications.



Note The **Services > Context Aware Notifications** page is available only in the root virtual domain.

This section contains the following topics:

- [Adding Event Groups, page 8-7](#)
- [Deleting Event Groups, page 8-7](#)

Adding Event Groups

To add an event group, follow these steps:

-
- Step 1** Choose **Services > Context Aware Notifications**.
 - Step 2** Choose **Notification Definitions**.
 - Step 3** From the Select a command drop-down list, choose **Add Event Group**. Click **Go**.
 - Step 4** Enter the name of the group in the Group Name text box.
 - Step 5** Click **Save**.

The new event group appears in the Event Settings page.

Deleting Event Groups

To delete an event group, follow these steps:

-
- Step 1** Choose **Services > Context Aware Notifications**.
 - Step 2** Choose **Notification Definitions**.
 - Step 3** Select the event group to delete by selecting its corresponding check box.
 - Step 4** From the Select a command drop-down list, choose **Delete Event Group(s)**. Click **Go**.
 - Step 5** Click **OK** to confirm deletion.

Step 6 Click **Save**.

Adding, Deleting, and Testing Event Definitions

An event definition contains information about the condition that caused the event, the assets to which the event applies, and the event notification destination.

This section describes how to add, delete, and test event definitions and contains the following topics:

- [Adding an Event Definition, page 8-8](#)
- [Deleting an Event Definition, page 8-12](#)
- [Testing Event Definitions, page 8-12](#)

Adding an Event Definition

The Prime Infrastructure enables you to add an event definition to a group. An event definition must belong to a particular group.

To add an event definition, follow these steps:

- Step 1** Choose **Services > Context Aware Notifications**.
- Step 2** From the left sidebar menu, choose **Notification Definitions**.
- Step 3** Click the name of the group to which you want to add an event definition. An event settings page appears showing existing event definitions for the event group.
- Step 4** From the Select a command drop-down list, choose **Add Event Definition**. Click **Go**.
- Step 5** On the Conditions tab, add one or more conditions. For each condition you add, specify the rules for triggering event notifications.



Tip For example, to keep track of heart monitors in a hospital, you might add rules to generate notifications when the following occur: (1) the heart monitor is missing for one hour, (2) the heart monitor moves off its assigned floor, or (3) the heart monitor enters a specific coverage area within a floor. In this example, add three separate rules to address these occurrences.

To add a condition, follow these steps:

- a. Click **Add** to add a condition that triggers a notification.
- b. In the Add/Edit Condition dialog box, follow these steps:
 1. Choose a condition type from the Condition Type drop-down list.
 - If you chose Missing from the Condition Type drop-down list, enter the number of minutes after which a missing asset generates a notification. For example, if you enter 10 in this text box, the mobility services engine generates a missing asset notification if the mobility services engine has not located the asset for more than 10 minutes after the device has become inactive or is no longer in the system. This condition occurs when the controller detects its absence and informs the mobility services engine about it, or if the mobility services engine does not hear anything about this device from the controller for 60 minutes by default. This value is only configurable

from the MSE command-line interface (accessible using `cmdshell` on the console) using the `config mobile-node-inactive-in-minutes` command for clients and `config tag-inactive-time-in-minutes` command for tags. Proceed to Step e.

- If you choose In/Out from the Condition Type drop-down list, choose **Inside of** or **Outside of**, then click **Select Area**. Entry and exit of assets from the selected area is then monitored. In the Select dialog box, choose the area to monitor, then click **Select**. The area to monitor can be an entire campus, building within a campus, a floor in a building, or a coverage area (you can define a coverage area using the map editor). For example, to monitor part of a floor in a building, choose a campus from the Campus drop-down list, choose a building from the Building drop-down list, and choose the area to monitor from the Floor Area drop-down list. Then click **Select**. Proceed to Step e.
- If you chose Distance from the Condition Type drop-down list, enter the distance in feet from a designated marker beyond which an asset triggers an event notification. Click **Select Marker**. In the Select dialog box, choose the campus, building, floor, and marker from the corresponding drop-down lists, and click **Select**. For example, if you add a marker to a floor plan and set the distance in the Trigger If text box to 60 feet, an event notification is generated if the monitored asset moves farther than 60 feet away from the marker. Proceed to Step e.



Note You can create markers and coverage areas using the Map Editor. When you create marker names, make sure they are unique across the entire system.

- If you chose Battery Level from the Condition Type drop-down list, select the check box next to the appropriate battery level (**low**, **medium**, **normal**) that triggers a notification. Proceed to Step e.
 - If you chose Location Change from the Condition Type drop-down list, proceed to Step e.
 - If you chose Emergency from the Condition Type drop-down list, click the button next to the appropriate emergency (**any**, **panic button**, **tampered**, **detached**) that triggers a notification. Proceed to Step e.
 - If you chose Chokepoint from the Condition Type drop-down list, proceed to Step c. There is only one trigger condition and it is displayed by default. No configuration required.
- c. In the Trigger If text box, specify the time in minutes to trigger the notification. The default is 60 minutes.
 - d. Select either **Recurring** or **Non-recurring** from the Notification Frequency radio button. If the frequency is non-recurring, the MSE sends absence notification only once. For recurring frequency, the MSE sends an absence notification periodically until the device becomes present again. Here period refers to the configured value in the absence definition.
 - e. From the Apply To drop-down list, choose the type of asset (**Any**, **Clients**, **Tags**, **Rogue APs**, **Rogue Clients**, or **Interferers**) for which a notification is generated if the trigger condition is met.



Note If you choose *Any* from the Apply to drop-down list, the battery condition is applied to all tags, clients, rogue access points, and rogue clients.



Note Emergency and chokepoint notifications apply only to Cisco-compatible extension (CX) tags Version 1 or later.

- f. The Match By drop-down list contains the following choices, from left to right:

- Choose the matching criteria (**MAC Address**, **Asset Name**, **Asset Group**, or **Asset Category**) from the first drop-down list.
- Choose the operator (**Equals** or **Like**) from the second drop-down list.
- Enter the relevant text into the text box based on the Match By criteria you chose.

The following examples describe the asset matching criteria that you can specify:

- If you choose **MAC Address** from the first drop-down list, choose **Equals** from the second drop-down list, and enter a MAC address (for example 12:12:12:12:12:12) in the text box, the event condition applies to the element whose MAC address is 12:12:12:12:12:12 (exact match).
- If you choose **MAC Address** from the first drop-down list, choose **Like** from the second drop-down list, and enter 12:12 in the text box, the event condition applies to elements whose MAC address starts with 12:12.



Note If the MAC address is a partial MAC address, then it might cause a performance issue in the Prime Infrastructure.

- g. Click **Add** to add the condition you have just defined.



Note If you are defining a chokepoint, you must select the chokepoint after you add the condition.

Defining a Chokepoint

To select a chokepoint, do the following:

- Step 1** Choose Chokepoint from the Condition Type drop-down list in the Add/Edit Condition dialog box.
- Choose Area type, Campus, and Outdoor Area from the appropriate drop-down lists.
 - Choose a Chokepoint from the menu that appears.
- The Add/Edit Condition dialog box reappears and the location path (*Campus > Building > Floor*) for the chokepoint auto-populates the entry text box next to the Select Checkpoint button.
- Step 2** On the Destination and Transport tab, follow these steps to add one or more destinations to receive event notifications and to configure the transport settings:
- To add a new destination, click **Add**. The Add/Edit Destination and Transport dialog box appears.
 - Click **Add New**.
 - In the dialog box that appears, enter the IP address or hostname of the system that receives event notifications, and click **OK**.
- The new entry is placed in the right column.
- The recipient system must have an event listener running to process notifications. By default, when you create an event definition, the Prime Infrastructure adds its IP address as the destination.
- To select a destination for notifications, highlight one or more IP addresses in the text area on the right, and click **Select** to add the IP addresses to the text area on the left.
 - From the Message Format radio button, select either **XML** or **Plain Text** as the message format.



Note If you select Prime Infrastructure as the destination for notifications, you must select the XML format.

- f. Choose one of the following transport types from the Transport Type drop-down list:
 - **SOAP**—Simple Object Access Protocol. Use SOAP to send notifications over HTTP/HTTPS and to be processed by web services on the destination.
Specify whether to send notifications over HTTPS by selecting its corresponding check box. Enter the destination port number in the Port Number text box.
 - **Mail**—Use this option to send notifications through e-mail.
Choose the protocol for sending the mail from the Mail Type drop-down list. Enter the following: username and password (if Authentication is enabled), name of the sender, prefix to add to the subject line, e-mail address of recipient, and a port number if necessary.
 - **SNMP**—Simple Network Management Protocol. Use this option to send notifications to SNMP-capable devices.
If you selected SNMP Version v2c, you are prompted to enter the SNMP community string in the SNMP Community text box and the applicable port number in the Port Number text box.
If you selected SNMP Version v3, you are prompted to enter the username, security name, choose the authentication type from the drop-down list, enter the authentication password, choose the privacy type from the drop-down list, and enter the privacy password.
 - **Syslog**—Specifies the system log on the destination system as the recipient of event notifications. Enter the notification priority in the Priority text box, the name of the facility, and the port number on the destination system.
- g. To enable HTTPS, select the **Enable** check box.
- h. The Port Number auto-populates.
- i. Click **Save**.

Step 3 On the General tab, follow these steps:

- a. Select the Admin Status **Enabled** check box to enable event definition (disabled by default).
- b. Set the event definition priority by choosing a number from the Priority drop-down list. Zero is highest.



Note An event definition with a higher priority is serviced before event definitions with a lower priority.

- c. Choose the frequency of notifications:
 1. Select the **All the Time** check box to continuously report events. Proceed to Step g.
 2. Unselect the **All the Time** check box to select the day and time of the week that you want event notifications sent. Days of the week and time text boxes appear for selection. Proceed to Step d.
- d. Select the check box next to each day that you want the event notification to be sent.
- e. From the Apply From drop-down list, choose a start time for the event notification. The possible values are hour, minute, and AM or PM.
- f. From the Apply Until drop-down list, choose an end time for the event notification. The possible values are selecting the hour, minute, and AM or PM.

The Prime Infrastructure shows a summary of event notifications for each of the seven event notification categories.



Note Emergency and chokepoint notifications are reported and displayed only for Cisco CX v.1-compliant tags.

Step 2 To view event notifications for a monitored asset, click one of its corresponding links. For example, to view absence events for client stations generated in the last hour, click the link in the Last Hour column for the Client Stations entry in the Absence (Missing) list.



CHAPTER 9

Context-Aware Service Planning and Verification

This chapter describes a number of tools and configurations that can be used to enhance the location accuracy of elements (clients, tags, rogue clients, interferers, and rogue access points) within an indoor or outdoor area.

This chapter contains the following sections:

- [Licensing Requirements, page 9-1](#)
- [Guidelines and Limitations, page 9-2](#)
- [Planning Data, Voice, and Location Deployment, page 9-2](#)
- [Calibration Models, page 9-3](#)
- [Inspecting Location Readiness and Quality, page 9-7](#)
- [Verifying Location Accuracy, page 9-8](#)
- [Using Optimized Monitor Mode to Enhance Tag Location Reporting, page 9-12](#)
- [Defining Inclusion and Exclusion Regions on a Floor, page 9-13](#)
- [Defining a Rail Line on a Floor, page 9-17](#)
- [Modifying Context-Aware Service Parameters, page 9-21](#)
- [Enabling Notifications and Configuring Notification Parameters, page 9-35](#)
- [Location Template for Controllers, page 9-38](#)
- [Location Services on Wired Switches and Wired Clients, page 9-40](#)
- [Verifying an NMSP Connection to a Mobility Services Engine, page 9-44](#)

Licensing Requirements

You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points. Licenses for tags and clients are offered separately. (The clients license also includes tracking of rogue clients and rogue access points).

For more information, see the *Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide* at http://www.cisco.com/en/US/products/ps9742/products_data_sheets_list.html.

For details on adding client and tag licenses to the mobility services engine, see [Chapter 2, “Adding and Deleting Mobility Services Engines and Licenses”](#).

Guidelines and Limitations

- Context-Aware Service (CAS) installed on a mobility services engine retrieves location information as well as other contextual information such as temperature and asset availability about a client or tag (Cisco CX Version 1 or later) from access points.
- Non-Cisco CX tags are not tracked or mapped by the Cisco Prime Infrastructure.
- Context-Aware Service was previously referred to as Cisco location-based services.

Planning Data, Voice, and Location Deployment

You can calculate the recommended number and location of access points based on the services (data, voice, location, or a combination) that are active.

This section contains the following topics:

- [Guidelines and Limitations, page 9-2](#)
- [Calculating the Placement of Access Points, page 9-2](#)

Guidelines and Limitations

- Access points, clients, and tags must be selected in the Floor Settings menu of the Monitor > Site MAPs page to appear on the map.
- Recommended calculations assume the need for consistently strong signals. In some cases, fewer access points may be required than recommended.
- You must select the Location Services to ensure that the recommended access points provide the true location of an element within 7 meters at least 90% of the time.

Calculating the Placement of Access Points

To calculate the recommended number and placement of access points on a floor, follow these steps:

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

The Site Map page appears.

Step 2 Click the appropriate map name link in the summary list that appears.

If you selected a building map, select a floor map in the Building View page.

A color-coded map appears showing placement of all installed elements (access points, clients, tags) and their relative signal strength.



Note The Access Points, Clients, and 802.11 Tags check boxes must be selected in the Floor Settings dialog box of the Monitor > Site Maps page to appear on the map.

Step 3 Choose **Planning Mode** from the Select a command drop-down list (top-right) and click **Go**.

A map appears with planning mode options at the top of the page.

Step 4 Click **Add APs**.

In the page that appears, drag the dashed rectangle over the map location for which you want to calculate the recommended access points.



Note Adjust the size or placement of the rectangle by selecting the edge of the rectangle and holding down the **Shift** key. Move the mouse as necessary to outline the targeted location.

Step 5 Select the check box next to the service that is used on the floor. The options are Data/Coverage (default), Voice, Location, and Location with Monitor Mode APs. Click **Calculate**.

The recommended number of access points appears.



Note Each service option includes all services that are listed above it. For example, if you select the Location check box, the calculation considers data/coverage, voice, and location in determining the number of access points required.

Step 6 Click **Apply** to generate a map based on the recommended number of access points and their proposed placement in the selected area.

Calibration Models

Information on Calibration Models

If the provided RF models do not sufficiently characterize your floor layout, you can create and apply a calibration model to your floor that better represents its attenuation characteristics. In environments in which many floors share common attenuation characteristics (such as in a library), you can create one calibration model and apply it to floors with the same physical layout and same deployment.

You can collect data for a calibration using one of two methods:

- Data point collection—Selects calibration points and calculates their coverage area one location at a time.
- Linear point collection—Selects a series of linear paths and then calculates the coverage area as you traverse the path. This approach is generally faster than data point collection. You can also employ data point collection to augment location data missed by the linear paths.

This section contains the following topics:

- [Guidelines and Limitations, page 9-3](#)
- [Creating and Applying Data Point and Calibration Models, page 9-4](#)

Guidelines and Limitations

- Calibration models can only be applied to clients, rogue clients, and rogue access points. Calibration for tags is done using the AeroScout System Manager. For more information on tag calibration, see the documentation available at the following URL: <http://support.aeroscout.com>.

- We recommend a client device that supports both 802.11a/n and 802.11b/g/n radios to expedite the calibration process for both spectrums.
- Use a laptop or other wireless device to open a browser to the Prime Infrastructure and perform the calibration process.
- Use only associated clients to collect calibration data.
- Rotate the calibrating client laptop during data collection so that the client is detected evenly by all access points in the vicinity.
- Do not stop data collection until you reach the endpoint even if the data collection bar indicates completion.
- It is generally observed that the point calibration gives more accurate calibration than line calibration.

Creating and Applying Data Point and Calibration Models

To create and apply data point and linear calibration models, follow these steps:

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

Step 2 From the Select a command drop-down list, choose **RF Calibration Models**. Click **Go**.

The RF Calibration Models page displays a list of calibration models. The default calibration model is available in all the virtual domains.

Step 3 From the Select a command drop-down list, choose **Create New Model**. Click **Go**.

Step 4 Assign a name to the model in the Model Name text box. Click **OK**.

The new model appears along with the other RF calibration models, but its status is listed as *Not yet calibrated*.

Step 5 To start the calibration process, click the **Model Name** link. A new page appears showing the details of the new model.



Note In this page, you can rename and delete the calibration model by choosing the proper option from the Select a command list drop-down list. When renaming the model, enter the new name before selecting **Rename Model**.

Step 6 From the Select a command drop-down list, choose **Add Data Points**, and click **Go**.

The campus, building, and floors displayed on this page are filtered based on the virtual domain.

Step 7 If you are performing this process from a mobile device connected to the Prime Infrastructure through the Cisco Centralized architecture, the MAC address text box is automatically populated with the address of the device. Otherwise, you can manually enter the MAC address of the device you are using to perform the calibration. MAC addresses that are manually entered must be delimited with colons (such as FF:FF:FF:FF:FF:FF).



Note If this process is being performed from a mobile device connected to the Prime Infrastructure through the Cisco Centralized architecture, the MAC address text box is automatically populated with the device address.

- Step 8** Choose the appropriate campus, building, floor, or outdoor area where the calibration is to be performed. Click **Next**.



Note The calibration in Outdoor Area is supported in Release 7.0.200.x and later. You can use this option to add the calibration data points to the outdoor area. The data points can be added to the Outdoor Area using the same procedure for calibration.

- Step 9** When the chosen floor map and access point locations appear, a grid of plus marks (+) indicates the locations where data is collected for calibration.

Using these locations as guidelines, you can perform either a point or linear data collection by appropriate placement of either the Calibration Point pop-up (point) or the Start and Finish pop-ups (linear) that appear on the map when the respective options appear.

- a. To perform a point collection, follow these steps:
1. From the Collection Method drop-down list, choose **Point**, and select the **Show Data Points** check box if not already selected. A Calibration Point pop-up menu appears on the map.
 2. Position the tip of the Calibration Point pop-up at a data point (+), and click **Go**. A page appears showing the progress of the data collection.
 3. When the data collection is complete for a selected data point and the coverage area is plotted on the map, move the Calibration Point pop-up to another data point, and click **Go**.



Note The coverage area plotted on the map is color coded and corresponds with the specific wireless LAN standard used to collect that data. Information on color-coding is provided in legend on the left sidebar menu. Additionally, the progress of the calibration process is indicated by two status bars above the legend, one for 802.11a/n and one for 802.11b/g/n.



Note To delete data points, click **Delete** and move the black square that appears over the appropriate data points. Resize the square as necessary by pressing **Ctrl** and moving the mouse.

4. Repeat point collection Steps a1 to a3 until the calibrations status bars of the relevant spectrums (802.11a/n, 802.11b/g/n) display as done.



Note The calibration status bar indicates data collection for the calibration as done, after at least 50 distinct locations and 150 measurements have been gathered. For every location point saved in the calibration process, more than one data point is gathered. The progress of the calibration process is indicated by two status bars above the legend, one for 802.11b/g/n and one for 802.11a/n.

- b. To perform a linear collection, follow these steps:
1. From the Collection Method drop-down list, choose **Linear** and select the **Show Data points** check box if not already selected. A line appears on the map with both Start and Finish pop-ups.
 2. Position the tip of the Start pop-up at the starting data point.
 3. Position the Finish pop-up at the ending data point.

4. Position yourself with your laptop at the starting data point, and click **Go**. Walk steadily towards the endpoint along the defined path. A dialog box appears to show that the data collection is in progress.



Note Do not stop data collection until you reach the endpoint even if the data collection bar indicates completion.

5. Press the space bar (or press **Done** in the data collection page) when you reach the endpoint. The collection dialog box shows the number of samples taken before it closes to reveal the map. The map displays all the coverage areas where data was collected.



Note To delete data points selected in error, click **Delete** and move the black square that appears over the appropriate data points. Resize the square as necessary by pressing **Ctrl** and moving the mouse.



Note The coverage area is color-coded and corresponds with the specific wireless LAN standard (802.11a/n, 802.11b/g/n, or 802.11a/b/g/n) used to collect that data (See legend in the left pane).

6. Repeat Steps b2 to b5 until the status bar for the respective spectrum is complete.



Note You can augment linear collection with data point collection to address missed coverage areas. See [Step 9 a](#).

Step 10 To calibrate the data points, click the name of the calibration model at the top of the page. The main page for that model appears.

Step 11 From the Select a command drop-down list, choose **Calibrate**, and click **Go**.

Step 12 Click **Inspect Location Quality** when calibration completes. A map appears showing RSSI readings.

Step 13 To use the newly created calibration model, you must apply the model to the floor on which it was created (and on any other floors with similar attenuation characteristics). Choose **Monitor > Site Maps** and find the floor. At the floor map interface, choose **Edit Floor Area** from the drop-down list, and click **Go**.

Step 14 From the Floor Type (RF Model) drop-down list, choose the newly created calibration model. Click **OK** to apply the model to the floor.



Note This process can be repeated for as many models and floors as needed. After a model is applied to a floor, all locations are determined using the specific collected attenuation data from the calibration model.

Inspecting Location Readiness and Quality

You can configure the Prime Infrastructure to verify the ability of an existing access point deployment to estimate the true location of a client, rogue client, rogue access point, or tag within 7 meters at least 90% of the time. Location readiness calculation is determined by the number and placement of access points.

This section contains the following topics:

- [Guidelines and Limitations, page 9-7](#)
- [Inspecting Location Readiness Using Access Point Data, page 9-7](#)
- [Inspecting Location Quality Using Calibration Data, page 9-8](#)

Guidelines and Limitations

Inspecting Location Readiness Using Access Point Data

By using data points gathered during a physical inspection and calibration, you can verify that a location meets the location specification (7 meters, 90%).

Inspecting Location Readiness Using Access Point Data

To inspect location readiness using access point data, follow these steps:

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

Step 2 Choose the appropriate floor location link from the list.

A map appears showing the placement of all installed access points, clients, and tags and their relative signal strength.



Note If RSSI is not displayed, you can enable AP Heatmaps by selecting the AP Heatmaps check box on the left sidebar menu.



Note If clients, 802.11 tags, access points, and interferers are not displayed, verify that their respective check boxes are selected on the left sidebar menu. Additionally, licenses for both clients and tags must be purchased for each of them to be tracked. For more information, see the *Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide* at http://www.cisco.com/en/US/products/ps9742/products_data_sheets_list.html.



Note See [Chapter 2, “Adding and Deleting Mobility Services Engines and Licenses,”](#) for details on installing client and tag licenses.

Step 3 From the Select a command drop-down list, choose **Inspect Location Readiness**, and click **Go**.

A color-coded map appears showing those areas that meet (indicated by Yes) and do not meet (indicated by No) the ten meter and 90% location specification.

Inspecting Location Quality Using Calibration Data

After completing a calibration model based on data points generated during a physical tour of the area, you can inspect the location quality of the access points.

To inspect location quality based on calibration, follow these steps:

-
- Step 1** Choose **Monitor > Site Maps**.
 - Step 2** From the Select a command drop-down list, choose **RF Calibration Model**. Click **Go**.
A list of defined calibration models appears.
 - Step 3** Click the appropriate calibration model.
Details on the calibration including date of last calibration, number of data points by signal type (802.11a, 802.11 b/g) used in the calibration, location, and coverage are displayed.
 - Step 4** Click the **Inspect Location Quality** link.
A color-coded map noting the percentage of location errors appears.



Note You can modify the distance selected to see the effect on the location errors.

Verifying Location Accuracy

By verifying location accuracy, you are ensuring that the existing access point deployment can estimate the location accuracy of the deployment.

You can analyze the location accuracy of non-rogue and rogue clients, asset tags, and interferers by using the Location Accuracy Tool.

The Location Accuracy Tool enables you to run either a scheduled or on-demand location accuracy test. Both tests are configured and executed through a single window.

There are two ways to test location accuracy using the Location Accuracy Tool:

- **Scheduled Accuracy Testing**—Employed when clients and tags are already deployed and associated to the wireless LAN infrastructure. Scheduled tests can be configured and saved when clients and tags are already pre-positioned so that the test can be run on a regularly scheduled basis.
- **On-Demand Accuracy Testing**—Employed when elements are associated but not pre-positioned. On demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy for a small number of clients, tags and interferers.

**Note**

The Accuracy Tool enables you to run either a scheduled or on-demand location accuracy test. Both tests are configured and executed through a single page.

This section contains the following topics:

- [Using Scheduled Accuracy Testing to Verify Current Location Accuracy, page 9-9](#)
- [Using On-Demand Location Accuracy Testing, page 9-10](#)

Using Scheduled Accuracy Testing to Verify Current Location Accuracy

To configure a scheduled accuracy test, follow these steps:

-
- Step 1** Choose **Tools > Location Accuracy Tool**.
- Step 2** From the Select a command drop-down list, choose **New Scheduled Accuracy Test**.
The campus, building, and floors are displayed on this page are filtered based on the virtual domain.
- Step 3** Enter a test name.
- Step 4** Choose an area type from the drop-down list.
- Step 5** Campus is configured as system campus by default. There is no need to change this setting.
- Step 6** Choose the building from the drop-down list.
- Step 7** Choose the floor from the drop-down list.
- Step 8** Select the begin and end time of the test by entering the days, hours, and minutes. Hours are represented using a 24-hour clock.

**Note**

When entering the test start time, be sure to allow enough time to position testpoints on the map prior to the test start.

- Step 9** Select the destination point for the test results. You can have the report e-mailed to you or you can download the test results from the Accuracy Tests > Results page. Reports are in PDF format.

**Note**

If you select the e-mail option, an SMTP mail server must first be defined for the target e-mail address. Choose **Administrator > Settings > Mail Server Configuration** to enter the appropriate information.

- Step 10** Click **Position Testpoints**. The floor map appears with a list of all clients and tags on that floor with their MAC addresses.
- Step 11** Select the check box next to each client and tag for which you want to check the location accuracy.

When you select the MAC address check box for a client or tag, two overlapping icons appear on the map for that element.

One icon represents the actual location and the other the reported location.



Note To enter a MAC address for a client or tag that is not listed, select the **Add New MAC** check box, enter the MAC address, and click **Go**. An icon for the element appears on the map. If the newly added element is on the mobility services engine but on a different floor, the icon appears in the left corner (0,0) position.

Step 12 If the actual location for an element is not the same as the reported location, drag the actual location icon for that element to the correct position on the map.



Note Only the actual location icon can be dragged.

Step 13 Click **Save** when all elements are positioned. A dialog box appears confirming successful accuracy testing.

Step 14 Click **OK** to close the confirmation page. You are returned to the Accuracy Tests summary page.



Note The accuracy test status appears as **Scheduled** when the test is about to execute. A status of **In Progress** appears when the test is running and **Idle** when the test is complete. A **Failure** status appears when the test is not successful.

Step 15 To view the results of the location accuracy test, click **Test name** and then click the **Results** tab in the page that appears.

Step 16 In the Results page, click the **Download** link under the Saved Report heading to view the report.

The Scheduled Location Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges
- An error distance histogram
- A cumulative error distribution graph
- An error distance over time graph
- A summary by each MAC address whose location accuracy was tested noting its actual location, error distance and a map showing its spatial accuracy (actual vs. calculated location) and error distance over time for each MAC.

Using On-Demand Location Accuracy Testing

An on-demand accuracy test is run when elements are associated but not pre-positioned. On-demand testing allows you to test the location accuracy of clients and tags at a number of different locations. You generally use it to test the location accuracy for a small number of clients and tags.

To run an on-demand accuracy test, follow these steps:

-
- Step 1** Choose **Tools > Location Accuracy Tool**.
- Step 2** From the Select a command drop-down list, choose **New On demand Accuracy Test**.
- Step 3** Enter a test name.
- Step 4** Choose the area type from the drop-down list.
- Step 5** Campus is configured as system campus by default. There is no need to change this setting.
- Step 6** Choose the building from the drop-down list.
- Step 7** Choose the floor from the drop-down list.
- Step 8** View the test results in the Accuracy Tests > Results page. Reports are in PDF format.
- Step 9** Click **Position Testpoints**. The floor map appears with red cross hairs at the (0,0) coordinate.
- Step 10** To test the location accuracy and RSSI of a location, choose either **client** or **tag** from the drop-down list on the left. A list of all MAC addresses for the chosen option (client or tag) appears in a drop-down list to its right.
- Step 11** Choose a MAC address from the drop-down list, move the red cross hairs to a map location, and click the mouse to place it.
- Step 12** Click **Start** to begin collecting accuracy data.
- Step 13** Click **Stop** to finish collecting data. You should allow the test to run for at least two minutes before clicking Stop.
- Step 14** Repeat [Step 10](#) to [Step 13](#) for each testpoint that you want to plot on the map.
- Step 15** Click **Analyze** when you are finished mapping the testpoints.
- Step 16** Click the **Results** tab in the page that appears.
- The on-demand accuracy report includes the following information:
- A summary location accuracy report that details the percentage of elements that fell within various error ranges
 - An error distance histogram
 - A cumulative error distribution graph
- Step 17** To download accuracy test logs from the Accuracy Tests summary page:
- a. Select the **listed test** check box and choose either **Download Logs** or **Download Logs for Last Run** from the Select a command drop-down list.
 - b. Click **Go**.
- The Download Logs option downloads the logs for all accuracy tests for the selected test(s).
- The Download Logs for Last Run option downloads logs for only the most recent test run for the selected test(s).
-

Using Optimized Monitor Mode to Enhance Tag Location Reporting

To optimize monitoring and location calculation of tags, you can enable TOMM (Tracking Optimized Monitor Mode) on up to four channels within the 2.4-GHz band (802.11b/g radio) of an access point. This allows you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

You must enable monitor mode at the access point level before you can enable TOMM and assign monitoring channels on the 802.11 b/g radio of the access point.

This section contains the following topics:

- [Guidelines and Limitations, page 9-12](#)
- [Optimizing Monitoring and Location Calculation of Tags, page 9-12](#)

Guidelines and Limitations

You can configure fewer than four channels for monitoring.

Optimizing Monitoring and Location Calculation of Tags

To optimize monitoring and location calculation of tags, follow these steps:

Step 1 Enable monitor mode on the access point, by following these steps:

- Choose **Configure** > **Access Point** > *AP Name*.
- Select **Monitor** as the AP Mode.



Note For more details, see to the *Cisco Wireless Control System Configuration Guide, Release 7.0* at the following URL:
http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

Step 2 Enable TOMM and assign monitoring channels on the access point radio, by following these steps:

- After enabling monitor mode at the access point level, choose **Configure** > **Access Points**.
- At the Access Points summary page, click the **802.11 b/g Radio** link for the access point on which monitor mode is enabled.
- In the Radio details page, disable Admin Status by unselecting the check box. This disables the radio.
- Select the **Enable TOMM** check box.
- Select up to four channels (Channel 1, Channel 2, Channel 3, Channel 4) on which you want the access point to monitor tags.



Note To eliminate a monitoring channel, choose **None** from the channel drop-down list.

- f. Click **Save**.
 - g. In the Radio parameters page, reenable the radio by selecting the **Admin Status** check box.
 - h. Click **Save**. The access point is now configured as a TOMM access point.
The AP Mode appears as Monitor in the Monitor > Access Points page.
-

Defining Inclusion and Exclusion Regions on a Floor

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

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

This section contains the following topics:

- [Guidelines and Limitations, page 9-13](#)
- [Defining an Inclusion Region on a Floor, page 9-14](#)
- [Defining an Exclusion Region on a Floor, page 9-16](#)

Guidelines and Limitations

Consider the following when configuring exclusion and inclusion areas:

- In the Prime Infrastructure, inclusion and exclusion regions are calculated only for clients.
- Inclusion and exclusion areas can be any polygon shape and must have at least three points.
- You can define only one inclusion region on a floor. By default, an inclusion region is defined for each floor when it is added to the Prime Infrastructure. The inclusion region is indicated by a solid aqua line and generally outlines the region.
- You can define multiple exclusion regions on a floor.
- Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

This might cause some of the devices to be located outside inclusion regions or inside exclusion regions till their location is calculated again.

- You must select the Location Regions option in the Floor Settings menu of the Monitor > Site Maps page for inclusion and exclusion regions to appear on the map.

Opening the Map Editor

Follow these steps to use the map editor:

-
- Step 1** Choose **Design > Site Map Design**.
 - Step 2** Click the desired campus. The Site Maps > Campus Name page appears.
 - Step 3** Click a campus and then click a building.

- Step 4** Click the desired floor area. The Site Maps > Campus Name > Building Name > Floor Area Name page appears.
- Step 5** From the Select a command drop-down list, choose **Map Editor**, and click **Go**. The Map Editor page appears.
-

Using the Map Editor to Draw Coverage Areas

If you have a building that is non-rectangular or you want to mark a non-rectangular area within a floor, you can use the map editor to draw a coverage area.

- Step 1** Add the floor plan if it is not already represented in the Prime Infrastructure.
- Step 2** Choose **Design > Site Maps**.
- Step 3** Click the Map Name that corresponds to the outdoor area, campus, building, or floor you want to edit.
- Step 4** From the Select a command drop-down list, choose **Map Editor**, and click **Go**.
- Step 5** In the Map Editor page, click the **Draw Coverage Area** icon on the toolbar.
A pop-up menu appears.
- Step 6** Enter the name of the area that you are defining. Click **OK**.
A drawing tool appears.
- Step 7** Move the drawing tool to the area you want to outline.
- Click the left mouse button to begin and end drawing a line.
 - When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page.
- The outlined area must be a closed object to appear highlighted on the map.
- Step 8** Click the **disk** icon on the toolbar to save the newly drawn area. Click the **Map Name** that corresponds to the outdoor area, campus, building, or floor you want to edit.
-

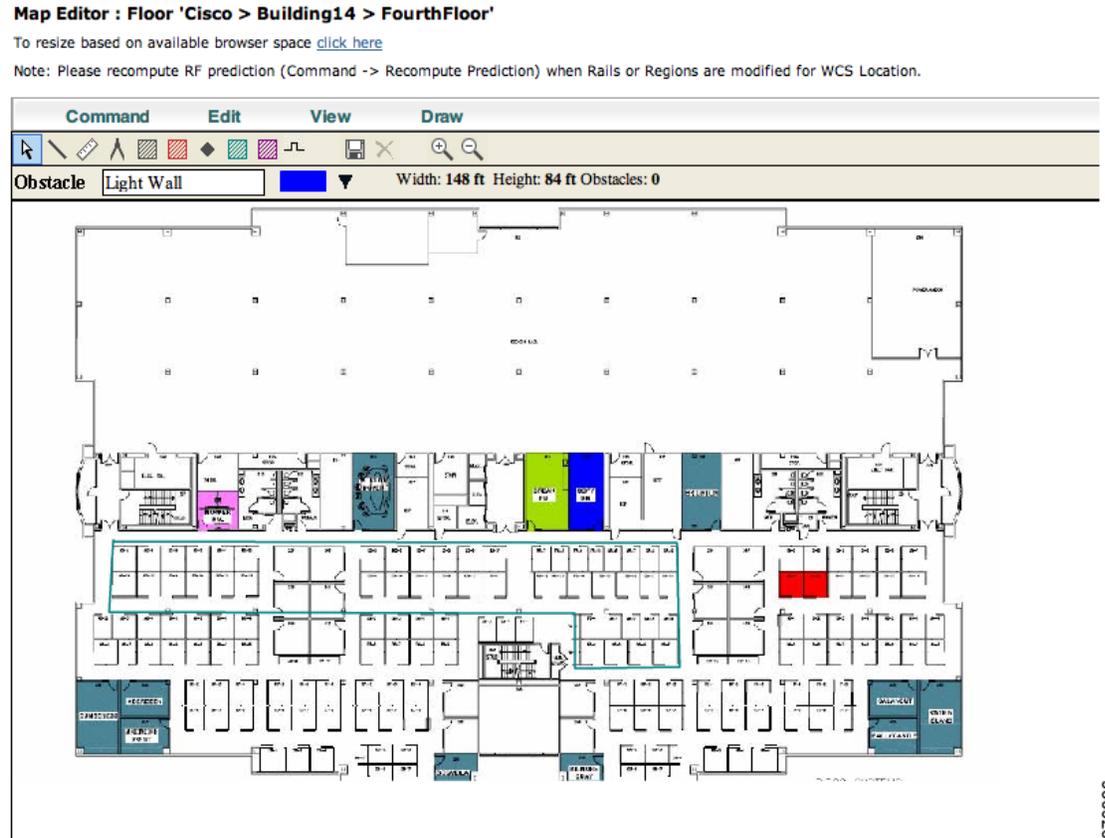
Defining an Inclusion Region on a Floor

To define an inclusion region, follow these steps:

- Step 1** Choose **Design > Site Maps**.
- Step 2** Click the name of the appropriate floor.
- Step 3** From the Select a command drop-down list, choose **Map Editor**, and click **Go**.
- Step 4** In the map, click the aqua box on the toolbar.
The Location Region Creation pop up window appears.
- Step 5** Select Inclusion from the Location Region Type drop-down list and click **OK**.
A drawing icon appears to outline the inclusion area.
- Step 6** To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.

- Step 7** Move the mouse cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line,
- Step 8** Repeat [Step 7](#) until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area (see [Figure 9-1](#)).

Figure 9-1 Inclusion Area Defined



- Step 9** Click the **disk** icon on the toolbar to save the inclusion region.



Note If you made an error in defining the inclusion area, you can edit the area using the Edit Mode option available. In the Next generation map editor, you can choose Edit Mode and click on the area to be edited and drag the vertices or hold down the mouse key and move the entire area to a different place.

- Step 10** Select the Location Regions check box if not already selected. If you want to apply it to all floor maps, click Save Settings. Close the Layers configuration page.
- Step 11** To resynchronize the Prime Infrastructure and MSE database, choose **Services > Synchronize Services**.



Note If two DBs are already synchronized, then a resynchronization happens automatically every time there is a change. There is no need for an explicit resynch.

Step 12 In the Synchronize Prime Infrastructure and MSE(s) page, click the **Network Designs** tab, and click **Synchronize**.

View the Sync. Status column to ensure that the synchronization is successful (two green arrows indicate success).

**Note**

- If the floor was already assigned previously to a mobility services engine, the changes on the floor are auto synchronized to the mobility services engine.
- For location calculation of an element, the rails and regions take effect only after the location is recalculated.
- Inclusion region configurations do not apply to tags.

**Note**

To delete an inclusion area, click the **Delete Mode** icon and select the region you want to delete and click the **Delete** button.

Defining an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define regions that are excluded (exclusion regions) in the calculations. Exclusion regions are generally defined within the borders of an inclusion region.

**Note**

Exclusion region configurations do not apply to tags.

To define an exclusion region, follow these steps:

- Step 1** Choose **Design > Site Maps**.
- Step 2** Click the name of the appropriate floor area.
- Step 3** From the Select a command drop-down list, choose **Map Editor**, and click **Go**.
- Step 4** In the map, click the purple box on the toolbar.
The Location Region Creation pop up window appears.
- Step 5** Select Exclusion from the Location Region Type drop-down list and click **OK**.
A drawing icon appears to outline the exclusion area.
- Step 6** To begin defining the exclusion area, move the drawing icon to the starting point on the map and click once.
- Step 7** Move the drawing icon along the boundary of the area you want to exclude and click once to start a boundary line and click again to end the boundary line.
- Step 8** Repeat [Step 7](#) until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple. when the area is completely defined. The excluded area is shaded in purple.
- Step 9** To define additional exclusion regions, repeat [Step 4](#) to [Step 8](#).
- Step 10** When all exclusion areas are defined, choose **Save** from the Command menu or click the disk icon on the toolbar to save the exclusion region.



Note To delete an exclusion area, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.

- Step 11** To return to the floor map to enable exclusion regions on heatmaps, choose **Exit** from the Command menu.
- Step 12** At the floor map, select the **Location Regions** check box if it is not already selected. The exclusion region is shown on the map.
- Step 13** To resynchronize the Prime Infrastructure and location databases, choose **Services > Synchronize Services**.
- Step 14** In the Synchronize page, from the Synchronize drop-down list, choose **Network Designs**, and then click **Synchronize**.

View the Sync. Status column to ensure that the synchronization is successful (two green arrows indicate success).



Note

- Exclusion region auto synchronizes with the mobility services engine if the floor was already synchronized to the mobility services engine.
 - You can draw multiple exclusion regions within an inclusion region.
 - For location calculation of an element, the rails and regions take effect only after the location is recalculated.
-

Defining a Rail Line on a Floor

You can define a rail line on a floor (such as a conveyor belt) that indicates an area where clients are expected to be.

Additionally, you can define an area (east and west or north and south) of the rail that expands the area that clients are expected to populate. This expanded area is known as the *snap-width* and further assists location calculations. Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority).

This section contains the following topics:

- [Guidelines and Limitations, page 9-17](#)
- [Defining a Rail on a Floor, page 9-18](#)

Guidelines and Limitations

- Rail line configurations do not apply to tags.
- Rails auto synchronize with the mobility services engine if the floor was already synchronized to the mobility services engine.
- For location calculation of an element, the rails and regions take effect only after the location is recalculated.

Defining a Rail on a Floor

The snap-width area is defined in feet or meters (user-defined).

To define a rail on a floor, follow these steps:

-
- Step 1** Choose **Monitor > Site Maps**.
 - Step 2** Click the name of the appropriate floor area.
 - Step 3** From the Select a command drop-down list, choose **Map Editor**, and click **Go**.
 - Step 4** Click the rail icon (to the right of the purple exclusion icon) on the toolbar.
 - Step 5** In the dialog box that appears, enter a snap-width (feet or meters) for the rail and then click **OK**.
 - Step 6** When the drawing icon appears, click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.
 - Step 7** Click the drawing icon twice when the rail line is completely drawn on the floor map. The rail line appears on the map and is bordered on both sides by the defined snap-width region.



Note To delete a rail line, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the *X* icon on the toolbar. The area is removed from the floor map.

- Step 8** To return to the floor map, choose the **Switch to floor view** icon.
- Step 9** In the floor map, select the **Rails** check box in the Floor Settings menu if it is not already selected. The rail is shown on the map.
- Step 10** To resynchronize the Prime Infrastructure and mobility services engine, choose **Services > Synchronize Services**.
- Step 11** In the Synchronize Services page, from the Synchronize drop-down list, choose **Network Designs** and then click **Synchronize**.

Look at the Sync. Status column to ensure that the synchronization is successful (two green arrows indicate success).

Adding an Outdoor Area



Note You can add an outdoor area to a campus map in the Prime Infrastructure database regardless of whether you have added outdoor area maps to the database.

To add an outdoor area to a campus map, follow these steps:

-
- Step 1** If you want to add a map of the outdoor area to the database, save the map in .PNG, .JPG, .JPEG, or .GIF format. Then browse to and import the map from anywhere in your file system.



Note You do not need a map to add an outdoor area. You can simply define the dimensions of the area to add it to the database. The map can be any size because the Prime Infrastructure automatically resizes the map to fit the workspace.

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

Step 3 Click the desired campus to display the Design > Site Maps > Campus View page.

Step 4 From the Select a command drop-down list, choose **New Outdoor Area**, and click **Go**.
The Create New Area page appears.

Step 5 In the New Outdoor Area page, enter the following information:

- Name—The user-defined name of the new outdoor area.
- Contact—The user-defined contact name.
- Area Type (RF Model)—Cubes And Walled Offices, Drywall Office Only, Outdoor Open Space (default).
- AP Height (feet)—Enter the height of the access point.
- Image File—Name of the file containing the outdoor area map. Click Browse to find the file.

Step 6 Click Next.

Step 7 Click **Place** to put the outdoor area on the campus map. The Prime Infrastructure creates an outdoor area rectangle scaled to the size of the campus map.

Step 8 Click and drag the outdoor area rectangle to the desired position on the campus map.

Step 9 Click **Save** to save this outdoor area and its campus location to the database.



Note A hyperlink associated with the outdoor area takes you to the corresponding Maps page.

Step 10 (Optional) To assign location presence information for the new outdoor area, choose **Edit Location Presence Info**, and click **Go**.



Note By default, the Override Child Element Presence Info check box is selected. There is no need to alter this setting for outdoor areas.

Configuring Interferer Notifications

You can configure this feature only from the campus, building, and floor view page.

To configure interferer notification, follow these steps:

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

Step 2 Click the name of the appropriate floor, building, or campus area.

Step 3 From the Select a command drop-down list, choose **Configure Interferer Notifications**, and click **Go**.
The Interferer CAS notification Configuration page appears. The following devices are displayed:

- Bluetooth Link
- Microwave Oven
- 802.11FH
- Bluetooth Discovery
- TDD Transmitter
- Jammer
- Continuous Transmitter
- DECT like Phone
- Video Camera
- 802.15.4
- WiFi Inverted
- WiFi Invalid channel
- Super AG
- Radar
- Canopy
- Xbox
- WiMAX Mobile
- WiMAX Fixed

Step 4 Select the devices check box for which you want notifications to be generated.

Step 5 Click **Save**.

Using Planning Mode

The planning mode opens the map editor in the browser window from which the planning tool is launched. If the original browser window has navigated away from the floor page, you need to navigate back to the floor page to launch the map editor.

You can calculate the recommended number and location of access points based on whether data and/or voice traffic and/or location are active.



Note

Based on the throughput specified for each protocol (802.11a or 802.11 b/g), planning mode calculates the total number of access points required that would provide optimum coverage in your network.

Planning Mode options:

- Add APs—Enables you to add access points on a map.
- Delete APs—Deletes the selected access points.
- Map Editor—Opens the Map Editor window. See the [“Defining Inclusion and Exclusion Regions on a Floor” section on page 9-13](#) for details.
- Synchronize with Deployment—Synchronizes your planning mode access points with the current deployment scenario.

- Generate Proposal—View a planning summary of the current access points deployment.
- Planned AP Association Tool—Allows you to add, delete, or import an AP Association from an Excel or CSV file. Once an access point is defined, it can be associated to a base radio MAC address using the Planned AP Association Tool. If the AP is not discovered, then they are pushed into a standby bucket and get associated when discovered.

**Note**

AP association is subjected to a limitation that AP should not belong to any floor or outdoor area. If the AP is already assigned to a floor or outdoor area, then the standby bucket holds the AP and, when removed from the floor or outdoor area, get positioned to the given floor. One MAC address cannot be put into a bucket for multiple floor or outdoor areas.

**Note**

The map synchronizations works only if the AP is associated to a base radio MAC address and not to its Ethernet MAC address.

Modifying Context-Aware Service Parameters

You can specify the type and number of clients or tags that are tracked and whether or not locations are calculated for those clients or tags.

You can also modify parameters that affect the location calculation of clients and tags such as Receiver Signal Strength Indicator (RSSI) measurements. Disable tracking and reporting of ad hoc rogue clients and access points.

This section contains the following topics:

- [Licensing Requirements, page 9-21](#)
- [Guidelines and Limitations, page 9-22](#)
- [Modifying Tracking Parameters, page 9-22](#)
- [Modifying Filtering Parameters, page 9-26](#)
- [Modifying History Parameters, page 9-28](#)
- [Enabling Location Presence, page 9-30](#)
- [Importing Asset Information, page 9-31](#)
- [Exporting Asset Information, page 9-32](#)
- [Modifying Location Parameters, page 9-32](#)

Licensing Requirements

Licenses are required to retrieve contextual information on tags and clients from access points. The license of the client also includes tracking of rogue clients and rogue access points. Licenses for tags and clients are offered independently and are offered in a range of quantities, from 3,000 to 12,000 units. For more information, see the *Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide* at http://www.cisco.com/en/US/products/ps9742/products_data_sheets_list.html.

Guidelines and Limitations

The Cisco 3315 Mobility Services Engine supports up to 2,000 clients and tags, and the Cisco 3350 Mobility Services Engine supports up to 18,000 clients and tags.

Modifying Tracking Parameters

The mobility services engine can track up to 18,000 clients (including rogue clients, rogue access points, wired clients, and interferers) and tags (combined count) with the proper license purchase and mobility services engine. Updates on the locations of tags, clients, and interferers being tracked are provided to the mobility services engine from the controller.

Only those tags, clients, and interferers that the controller is tracking are seen in the Prime Infrastructure maps, queries, and reports. No events and alarms are collected for non-tracked elements and none are used in calculating the 18,000 element limit for clients or tags.

You can modify the following tracking parameters using the Prime Infrastructure:

- Enable and disable wired and wireless client stations, active asset tags, and rogue clients, interferers, and access points whose locations you actively track.

Wired client location tracking enables servers in a data center to more easily find wired clients in the network. Servers are associated with wired switch ports in the network.

- Set limits on how many of a specific element you want to track.

For example, given a client license of 12,000 trackable units, you can set a limit to track only 8,000 client stations (leaving 4,000 units available to allocate between rogue clients and rogue access points). Once the tracking limit is met for a given element, the number of elements not being tracked is summarized in the Tracking Parameters page.

This section contains the following topics:

- [Guidelines and Limitations, page 9-22](#)
- [Configuring Tracking Parameters for a Mobility Services Engine, page 9-22](#)

Guidelines and Limitations

- When upgrading mobility services engines from Release 6.0 to 7.0, if any limits have been set on wireless clients or rogues, they are reset because of the wired client limit change in Release 7.0.
- The actual number of tracked clients is determined by the license purchased.
- The actual number of tracked active RFID tags is determined by the license purchased.
- We recommend that you use a Release 4.2 or higher controller for better latency and accuracy.

Configuring Tracking Parameters for a Mobility Services Engine

To configure tracking parameters for a mobility services engine, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engine**. The Mobility Services page appears.
- Step 2** Click the name of the mobility services engine whose properties you want to edit. The General Properties page appears.

- Step 3** Choose **Context Aware Service > Administration > Tracking Parameters** to display the configuration options.
- Step 4** Modify the tracking parameters as appropriate. [Table 9-1](#) lists the tracking parameters.

Table 9-1 Tracking Parameters

Field	Configuration Options
Tracking Parameters	
Wired Clients	<ol style="list-style-type: none"> Select the Enable check box to enable tracking of client stations by the mobility services engine. <p>In Release 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers.</p> <p>The wired client limiting is supported from mobility services engine 7.0 and Prime Infrastructure Release 7.0 and later. In other words, you can limit wired clients to a fixed number such as 500. This limit is set to ensure that the licenses are not taken up completely by wired clients and some licenses are available for wireless clients.</p> <div style="text-align: center;">  </div> <p>Caution When upgrading the mobility services engine from Release 6.0, if any limits have been set on wireless clients or rogues, they are reset because of the wired client limit change in Release 7.0.</p> <p>Note Active Value (Display only): Indicates the number of wired client stations currently being tracked.</p> <p>Note Not Tracked (Display only): Indicates the number of wired client stations beyond the limit.</p>
Wireless Clients	<ol style="list-style-type: none"> Select the Enable check box to enable tracking of client stations by the mobility services engine. Select the Enable Limiting check box to set a limit on the number of client stations to track. Enter a Limit Value if limiting is enabled. The limit entered can be any positive value up to 18,000 which is the maximum number of clients that can be tracked by a mobility services engine. <p>Note Active Value (Display only): Indicates the number of client stations currently being tracked.</p> <p>Note Not Tracked (Display only): Indicates the number of client stations beyond the limit.</p>

Table 9-1 Tracking Parameters (continued)

Field	Configuration Options
Rogue Access Points	<ol style="list-style-type: none"> 1. Select the Enable check box to enable tracking of rogue access points by the mobility services engine. 2. Select the Enable Limiting check box to set a limit on the number of rogue access points to track. 3. Enter a Limit Value if limiting is enabled. The limit entered can be any positive value up to 18,000 which is the maximum number of rogue access points that can be tracked by a mobility services engine. <p>Note Active Value (Display only): Indicates the number of rogue access points currently being tracked.</p> <p>Note Not Tracked (Display only): Indicates the number of rogue access points beyond the limit.</p>
Exclude Ad-Hoc Rogues	Select the check box to turn off the tracking and reporting of ad hoc rogues in the network. As a result, ad hoc rogues are not displayed on Prime Infrastructure maps or its events and alarms reported.
Rogue Clients	<ol style="list-style-type: none"> 1. Select the Enable check box to enable tracking of rogue clients by the mobility services engine. 2. Select the Enable Limiting check box to set a limit on the number of rogue clients to track. 3. Enter a Limit Value if limiting is enabled. The limit entered can be any positive value up to 18,000 which is the maximum number of rogue clients that can be tracked by a mobility services engine. <p>Note Active Value (Display only): Indicates the number of rogue clients being tracked.</p> <p>Note Not Tracked (Display only): Indicates the number of rogue clients beyond the limit.</p>
Interferers	<ol style="list-style-type: none"> 1. Select the Enable check box to enable tracking of the interferers by the mobility services engine. 2. Select the Enable Limiting check box to set a limit on the number of interferers to track. 3. Enter a Limit Value if limiting is enabled. <p>In Release 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers.</p> <p>In Release 7.0.200.x, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, interferers, and guests.</p> <p>Note Active Value (Display only): Indicates the number of interferers currently being tracked.</p> <p>Note Not Tracked (Display only): Indicates the number of interferers beyond the limit.</p>

Asset Tracking Elements

Table 9-1 Tracking Parameters (continued)

Field	Configuration Options
Active RFID Tags	<p>Select the Enable check box to enable tracking of active RFID tags by the mobility services engine.</p> <p>Note The actual number of tracked active RFID tags is determined by the license purchased.</p> <p>Note Active Value (Display only): Indicates the number of active RFID tags currently being tracked.</p> <p>Note Not Tracked (Display only): Indicates the number of active RFID tags beyond the limit.</p>
SNMP Parameters—Not applicable for controllers Release 4.2 and earlier. Also not applicable for MSEs 7.0.105.0 and later release.	
SNMP Retry Count	Enter the number of times to retry a polling cycle. The default value is 3. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier and location server Release 3.0 and earlier only.)
SNMP Timeout	Enter the number of seconds before a polling cycle times out. The default value is 5. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier and location server Release 3.0 and earlier only.)
SNMP Polling Interval—Not applicable for MSEs Release 7.0.105.0 and later.	
Client Stations	Select the Enable check box to enable client station polling and enter the polling interval in seconds. The default value is 300. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier and location server Release 3.0 and earlier only.)
Active RFID Tags	<p>Select the Enable check box to enable active RFID tag polling and enter the polling interval in seconds. Allowed values are from 1 to 99999.</p> <p> Note Before the mobility service can collect asset tag data from controllers, you must enable the detection of active RFID tags using the config rfid status enable command on the controllers.</p>
Rogue Clients and Access Points	Select the Enable check box to enable rogue access point polling and enter the polling interval in seconds. The default value is 600. Allowed values are from 1 to 99999 (Configurable in controller Release 4.1 and earlier and location server Release 3.0 and earlier only.)
Statistics	Select the Enable check box to enable statistics polling for the mobility service, and enter the polling interval in seconds. The default value is 900. Allowed values are from 1 to 99999 (Configurable in controller Release 4.1 and earlier and location server Release 3.0 and earlier only.)

Step 5 Click **Save** to store the new settings in the mobility services engine database.

Modifying Filtering Parameters

In addition to tracking parameters, you can use filtering to limit the number of clients, asset tags, wired clients, rogue clients, interferers, and access points whose locations are tracked. You can filter by MAC address and probing clients.

- MAC addresses

Specific MAC addresses can be entered and labeled as allowed or disallowed from location tracking. You can import a file with the MAC addresses that are to be allowed or disallowed, or you can enter them individually in the Prime Infrastructure.

The format for entering MAC addresses is xx:xx:xx:xx:xx:xx. If a file of MAC addresses is imported, the file must follow a specific format:

- Each MAC address should be listed on a separate line.
- Allowed MAC addresses must be listed first and preceded by an “[Allowed]” line item. Disallowed MAC addresses must be preceded by “[Disallowed].”
- Wildcard listings can be used to represent a range of MAC addresses. For example, the first entry “00:11:22:33:*” in the following allowed listing is a wildcard.



Note Allowed MAC address formats are viewable in the Filtering Parameters configuration page. See [Table 9-2](#) for details.

EXAMPLE file listing:

```
[Allowed]
00:11:22:33:*
22:cd:34:ae:56:45
02:23:23:34:*
[Disallowed]
00:10:*
ae:bc:de:ea:45:23
```

- Probing clients

Probing clients are clients that are associated with one controller but whose probing activity enables them to appear to another controller and count as an element for the *probed* controller as well as its primary controller.

This section contains the following topics:

- [Guidelines and Limitations, page 9-26](#)
- [Configuring Filtering Parameters for a Mobility Services Engine, page 9-26](#)

Guidelines and Limitations

Excluding probing clients can free up the licenses for the associated clients.

Configuring Filtering Parameters for a Mobility Services Engine

To configure filtering parameters for a mobility services engine, follow these steps:

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

- Step 2** Click the name of the mobility services engine whose properties you want to edit. The General Properties page appears.
- Step 3** Choose **Context Aware Service > Administration > Filtering Parameters** to display the configuration options.
- Step 4** Modify the filtering parameters as appropriate. [Table 9-2](#) lists filtering parameters.

Table 9-2 *Filtering Parameters*

Field	Configuration Options
Advanced Filtering Params	
Duty Cycle Cutoff Interferers	<p>Enter the duty cycle cutoff value for interferers so that only those interferers whose duty cycle meets the specified limits are tracked and counted against the CAS license.</p> <p>The default value for the Duty Cycle Cutoff Interferers is 0% and the configurable range is from 0% to 100%.</p> <p>In order to better utilize the location license, you can chose to specify a filter for interferers based on the duty cycle of the interferer.</p>
MAC Filtering Params	

Table 9-2 Filtering Parameters (continued)

Field	Configuration Options
Exclude Probing Clients	Select the check box to prevent calculating location for probing clients.
Enable Location MAC Filtering	<ol style="list-style-type: none"> 1. Select the check box to enable filtering of specific elements by their MAC addresses. 2. To import a file of MAC addresses (Upload a file for Location MAC Filtering text box), browse for the file name and click Save to load the file. MAC addresses from the list auto-populate the Allowed List and Disallowed List based on their designation in the file. <p>Note To view allowed MAC address formats, click the red question mark next to the Upload a file for Location MAC Filtering text box.</p> <ol style="list-style-type: none"> 3. To add an individual MAC address, enter the MAC addresses (format is xx:xx:xx:xx:xx:xx) in the Add a single MAC entry and click either Allow or Disallow. The address appears in the appropriate column. <p>Note To move an address between the Allow and Disallow columns, highlight the MAC address entry and click the button under the appropriate column.</p> <p>Note To move multiple addresses, click the first MAC address and then press Ctrl and click additional MAC addresses. Click Allow or Disallow to place an address in that column.</p> <p>Note If a MAC address is not listed in the Allow or Disallow column, it appears in the Blocked MACs column by default. If you click the Unblock button, the MAC address automatically moves to the Allow column. You can move it to the Disallow column by clicking the Disallow button under the Allow column.</p>

Step 5 Click **Save** to store the new settings in the mobility services engine database.

Modifying History Parameters

You can use the Prime Infrastructure to specify how long to store (archive) histories on client stations, asset tags, and rogue clients, wired clients, interferers and access points.

You can also program the mobility services engine to periodically prune (remove) duplicate data from its historical files, which increases the amount of memory available for storing the latest history information. This is important to prevent losing the latest history information due to lack of disk space.

Configuring Mobility Services Engine History Settings

To configure mobility services engine history, follow these steps:

- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the mobility services engine whose properties you want to edit.
- Step 3** Choose **Context Aware Service > Administration > History Parameters**.
- Step 4** Modify the following history parameters as appropriate. [Table 9-3](#) lists history parameter.

Table 9-3 History Parameters

Field	Description
Archive for	Enter the number of days for the location server to retain a history of each enabled category. Default value is 30. Allowed values are from 1 to 365.
Prune data starting at	Enter the number of hours and minutes at which the location server starts data pruning (between 0 and 23 hours, and between 1 and 59 minutes). Enter the interval in minutes after which data pruning starts again (between 1 and 99900000). Default start time is 23 hours and 50 minutes, and the default interval is 1440 minutes. Note Enter the default limits for better performance.
Client Stations	Select the Enable check box to turn on historical data collection for client stations.
Wired Stations	Select the Enable check box to turn on historical data collection for wired stations.
Asset Tags	Select the Enable check box to turn on historical data collection.  Note Before the mobility service can collect asset tag data from controllers, you must enable the detection of RFID tags using the config rfid status enable command.
Rogue Clients and Access Points	Select the Enable check box to turn on historical data collection.
Interferers	Select the Enable check box to turn on historical data collection.

- Step 5** Click **Save** to store your selections in the mobility services engine database.

Enabling Location Presence

You can enable location presence on a mobility services engine to expand civic (city, state, postal code, country) and geographic (longitude, latitude) location information beyond the Cisco default settings (campus, building, floor, and X, Y coordinates). You can then request this information for wireless and wired clients on demand for use by location-based services and applications.

You can also import advanced location information such as the MAC address of a wired client and the wired switch slot and port to which the wired client is attached.

You can configure location presence when a new campus, building, floor or outdoor area is added or configure it at a later date.

Once enabled, the mobility services engine can provide any requesting Cisco CX v5 client its location.



Note

Before enabling this feature, synchronize the mobility services engine.

This section contains the following topics:

- [Guidelines and Limitations, page 9-30](#)
- [Enabling and Configuring Location Presence on a Mobility Services Engine, page 9-30](#)

Guidelines and Limitations

For details on configuring location presence when adding a new campus, building, floor, or outdoor area, see Chapter 6, “Configuring Maps” section of the *Cisco Wireless Control System Configuration Guide*, Release 6.0.

Before enabling location presence, synchronize the mobility services engine.

Enabling and Configuring Location Presence on a Mobility Services Engine

To enable and configure location presence on a mobility services engine, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**. Select the mobility services engine to which the campus or building or floor is assigned.
 - Step 2** Choose **Context Aware Service > Administration > Presence Parameters**. The Presence page appears.
 - Step 3** Select the **Service Type On Demand** check box to enable location presence for Cisco CX clients v5.
 - Step 4** Select one of the following Location Resolution options:
 - a. When Building is selected, the mobility services engine can provide any requesting client its location by building.
 - For example, if a client requests its location and the client is located in Building A, the mobility services engine returns the client address as Building A.
 - b. When AP is selected, the mobility services engine can provide any requesting client its location by its associated access point. The MAC address of the access point appears.
 - For example, if a client requests its location and the client is associated with an access point with a MAC address of 3034:00hh:0adg, the mobility services engine returns the client address of 3034:00hh:0adg.

- c. When X,Y is selected, the mobility services engine can provide any requesting client its location by its X and Y coordinates.
 - For example, if a client requests its location and the client is located at (50, 200) the mobility services engine returns the client address of 50, 200.
- Step 5** Select any or all of the location formats check boxes:
- a. Select the **Cisco** check box to provide location by campus, building, floor, and X and Y coordinates. This is the default setting.
 - b. Select the **Civic** check box to provide the name and address (street, city, state, postal code, country) of a campus, building, floor, or outdoor area.
 - c. Select the **GEO** check box to provide the longitude and latitude coordinates.
- Step 6** By default, the Text check box for Location Response Encoding is selected. It indicates the format of the information when received by the client. There is no need to change this setting.
- Step 7** Select the **Retransmission Rule Enable** check box to allow the receiving client to retransmit the received information to another party.
- Step 8** Enter a Retention Expiration value in minutes. This determines how long the received information is stored by the client before it is overwritten. The default value is 24 hours (1440 minutes).
- Step 9** Click **Save**.
-

Importing and Exporting Asset Information

This section contains the following topics:

- [Importing Asset Information, page 9-31](#)
- [Exporting Asset Information, page 9-32](#)

Importing Asset Information

To import asset, chokepoint, and Time Difference Of Arrival (TDOA) receiver information for the mobility services engine using the Prime Infrastructure, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the mobility services engine for which you want to import information.
- Step 3** Choose **Context Aware Service > Administration > Import Asset Information**.
- Step 4** Enter the name of the text file or browse for the filename.
Specify information in the imported file in the following formats:
- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
 - station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname
- Step 5** Click **Import**.
-

Exporting Asset Information

To export asset, chokepoint, and Time Difference Of Arrival (TDOA) receiver information from the mobility services engine to a file using Prime Infrastructure, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the mobility services engine from which you want export information.
- Step 3** Choose **Context Aware Service > Administration > Export Asset Information**.
Information in the exported file is in the following formats:
- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
 - station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname
- Step 4** Click **Export**.
- Step 5** Click **Open** (display to page), **Save** (to external PC or server), or **Cancel**.



Note If you click **Save**, you are asked to select the asset file destination and name. The file is named assets.out by default. Click **Close** from the dialog box when download is complete.

Modifying Location Parameters

You can use the Prime Infrastructure to modify parameters that affect location calculations such as Receiver Signal Strength Indicator (RSSI) measurements for clients.

You can also apply varying smoothing rates to manage location movement of a client.

This section contains the following topics:

- [Guidelines and Limitations, page 9-32](#)
- [Configuring Location Parameters, page 9-32](#)

Guidelines and Limitations

- Location parameters apply only to clients.
- Enable the Calculation time parameter only under Cisco TAC personnel guidance because it slows down the overall location calculations.
- Modify the RSSI Cutoff parameter only under Cisco TAC personnel guidance. Modifying this value can reduce the location calculation accuracy.

Configuring Location Parameters

To configure location parameters, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the mobility services engine whose properties you want to modify.

- Step 3** Choose **Context Aware Service > Advanced > Location Parameters**. The configuration options appear.
- Step 4** Modify the location parameters as appropriate. [Table 9-4](#) lists location parameters.

Table 9-4 Location Parameters

Field	Configuration Options
Enable Calculation time	<p>Select the Enable check box to initiate the calculation of the time required to compute location.</p> <p>Note This parameter applies only to clients, rogue access points, rogue clients, and interferers.</p> <p> Caution Enable this parameter only under Cisco TAC personnel guidance because it slows down the overall location calculations.</p>
Enable OW Location	<p>Select the Enable check box to include Outer Wall (OW) calculation as part of location calculation.</p> <p>Note This parameter is ignored by the mobility services engine.</p>
Relative discard RSSI time	<p>Enter the number of minutes since the most recent RSSI sample after which RSSI measurement should be considered discarded. For example, if you set this parameter to 3 minutes and the mobility services engine receives two samples at 10 and 12 minutes, it keeps both samples. An additional sample received at 15 minutes is discarded. The default value is 3. Allowed values range from 0 to 99999. A value of less than 3 is not recommended.</p> <p>Note This parameter applies only to clients, rogue access points, rogue clients, and interferers.</p>
Absolute discard RSSI time	<p>Enter the number of minutes after which RSSI measurement should be considered stale and discarded, regardless of the most recent sample. The default value is 60. Allowed values range from 0 to 99999. A value of less than 60 is not recommended.</p> <p>Note This parameter applies only to clients.</p>
RSSI Cutoff	<p>Enter the RSSI cutoff value, in decibels (dBs) with respect to one (1) mW (dBm), above which the mobility services engine will always use the access point measurement. The default value is -75.</p> <p>Note When 3 or more measurements are available above the RSSI cutoff value, the mobility services engine discards any weaker values (lower than RSSI cutoff value) and use the 3 (or more) strongest measurements for calculation; however, when only weak measurements below the RSSI cutoff value are available, those values are used for calculation.</p> <p>Note This parameter applies only to clients.</p> <p> Caution Modify only under Cisco TAC personnel guidance. Modifying this value can reduce the accuracy of location calculation.</p>
Enable Location Filtering	<p>Location filtering is used to smooth out the jitters in the calculated location. This prevents the located device from jumping between two discrete points on the floor map.</p>

Table 9-4 Location Parameters (continued)

Field	Configuration Options
Chokepoint Usage	Select the Enable check box to enable chokepoints to track Cisco compatible tags.
Use Chokepoints for Interfloor conflicts	Perimeter chokepoints or weighted location readings can be used to locate Cisco compatible tags. Options: <ul style="list-style-type: none"> • Never: When selected, perimeter chokepoints are not used to locate Cisco compatible tags. • Always: When selected, perimeter points are used to locate Cisco compatible tags. • Floor Ambiguity: When selected, both weighted location readings and perimeter chokepoints are used to locate Cisco-compatible tags. If similar locations are calculated by the two methods, the perimeter chokepoint value is used by default.
Chokepoint Out of Range timeout	When a Cisco compatible tag leaves a chokepoint range, the timeout period entered is the period that passes before RSSI values are again used for determining location.
Absent Data cleanup interval	Enter the number of minutes that data for <i>absent</i> mobile stations is kept. An <i>absent</i> mobile station is one that was discovered but does not appear in the network. Default value is 1440.
Use Default Heatmaps for Non Cisco Antennas	Select this check box to enable the usage of default heatmaps for non-Cisco antennas during the Location Calculation. This option is disabled by default.
Movement Detection	
Individual RSSI change threshold	This parameter specifies the Individual RSSI movement recalculation trigger threshold. Enter a threshold value between 0-127 dBm. Modify only under Cisco TAC personnel guidance.
Aggregated RSSI change threshold	This parameter specifies the Aggregated RSSI movement recalculation trigger threshold. Enter a threshold value between 0-127 dBm. Modify only under Cisco TAC personnel guidance.
Many new RSSI change percentage threshold	This parameter specifies Many new RSSI movement recalculation trigger threshold in percentage. Modify only under Cisco TAC personnel guidance.
Many missing RSSI percentage threshold	This parameter specifies Many many RSSI movement recalculation trigger threshold in percentage. Modify only under Cisco TAC personnel guidance.

Step 5 Click **Save**.

Enabling Notifications and Configuring Notification Parameters

You can use the Prime Infrastructure to enable notifications and configure notification parameters.

This section contains the following topics:

- [Guidelines and Limitations, page 9-35](#)
- [Enabling Notifications, page 9-35](#)
- [Configuring Notification Parameters, page 9-35](#)
- [Viewing Notification Statistics, page 9-37](#)

Guidelines and Limitations

Modify notification parameters only when you expect the mobility services engine to send a large number of notifications or when notifications are not being received.

Enabling Notifications

You can use Prime Infrastructure to define and enable user-configured conditional notifications and northbound notifications.

User-configured conditional notifications manage which notifications the mobility services engine sends to the Prime Infrastructure or a third-party destination compatible with the mobility services engine notifications. See the [“Adding, Deleting, and Testing Event Definitions”](#) section on page 8-8.

Northbound notifications define which tag notifications the mobility services engine sends to third-party applications. Client notifications are not forwarded. By enabling northbound notifications in the Prime Infrastructure, the following five event notifications are sent: chokepoints, telemetry, emergency, battery, and vendor data. To send a tag location, you must enable that notification separately.

The mobility services engine sends all northbound notifications in a set format. Details are available on the Cisco developers support portal at the following URL:

<http://developer.cisco.com/web/cdc>

Configuring Notification Parameters

You can limit the rate at which a mobility services engine generates notifications, set a maximum queue size for notifications, and set a retry limit for notifications with in a certain period.

Notification parameter settings apply to user-configurable conditional notifications and northbound notifications except as noted in [Table 9-5](#).



Note

Modify notification parameters only when you expect the mobility services engine to send a large number of notifications or when notifications are not being received.

To enable northbound notifications and to configure notification parameters, follow these steps:

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

- Step 2** Click the name of the mobility services engine you want to configure.
- Step 3** Choose **Context Aware Service > Advanced > Notification Parameters** to display the configuration options.
- Step 4** Select the **Enable Northbound Notifications** check box to enable the function.
- Step 5** Select the **Notification Contents** check box to send notifications to third-party applications (northbound).
- Step 6** Select one or more of the following Notification Contents check boxes:
- **Chokepoints**
 - **Telemetry**
 - **Emergency**
 - **Battery Level**
 - **Vendor Data**
 - **Location**
- Step 7** Select the **Notification Triggers** check box.
- Step 8** Select one or more of the following Notification Triggers check boxes:
- **Chokepoints**
 - **Telemetry**
 - **Emergency**
 - **Battery Level**
 - **Vendor Data**
 - **Location Recalculation**
- Step 9** Enter the IP address or hostname and port for the system that is to receive the northbound notifications.
- Step 10** Choose the transport type from the drop-down list.
- Step 11** Select the **HTTPS** check box if you want to use HTTPS protocol for secure access to the destination system.
- Step 12** To modify the notification parameter settings, enter the new value in the appropriate text box in the Advanced tab of this page. See [Table 9-5](#).

Table 9-5 *User-Configurable Conditional and Northbound Notifications Fields*

Field	Configuration Options
Rate Limit	Enter the rate, in milliseconds, at which the mobility services engine generates notifications. A value of 0 (default) means that the mobility services engine generates notifications as fast as possible (Northbound notifications only).
Queue Limit	Enter the event queue limit for sending notifications. The mobility services engine drops any event above this limit. Default values: Cisco 3350 (30000), Cisco 3315 (5,000), and Cisco 2710 (10,000).
Retry Count	Enter the number of times to generate an event notification before the refresh time expires. This parameter can be used for asynchronous transport types which do not acknowledge the receipt of the notification and there is a possibility that the notification may be lost in transit. Default value is 1.
	Note The mobility services engine does not store events in its database.

Table 9-5 *User-Configurable Conditional and Northbound Notifications Fields (continued)*

Field	Configuration Options
Refresh Time	Enter the wait time in minutes that must pass before a notification is resent. For example, if a device is configured for In Coverage Area notification and it is constantly being detected within the Coverage Area. The notification is sent once every refresh time. Default value is 0 minutes.
Drop Oldest Entry on Queue Overflow	(Read-only). The number of event notifications dropped from the queue since startup.
Serialize Events per Mac address per Destination	Select this option if you want the successive events for the same MAC address to be sent to a single destination in a serial manner.

Step 13 Click **Save**.

Viewing Notification Statistics

You can view the notification statistics for a specific mobility engine. To view notification statistics information for a specific mobility services engine, follow these steps:

- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the mobility services engine you want to configure.
- Step 3** Choose **Context Aware Service > Advanced > Notification Parameters** to display the configuration options.

You can view the notification statistics for a specific mobility services engine. To view the Notification parameters, choose **Services > Mobility Services Engines > MSE-name > Context Aware Service > Notification Statistics**.

where *MSE-name* is the name of a mobility services engine.

[Table 9-6](#) describes the fields in the Notification Statistics page.

Table 9-6 *Notification Statistics Page Fields*

Field	Description
Summary	
Destinations	
Total	Destination total count.
Unreachable	Unreachable destination count.
Notification Statistics Summary	
Track Definition Status	Status of the track definition. Track notification status can be either Enabled or Disabled.
Track Definition	Track definition can be either Nothbound or CAS event notification.

Table 9-6 Notification Statistics Page Fields (continued)

Field	Description
Summary	
Destination IP Address	The destination IP address to which the notifications are sent.
Destination Port	The destination port to which the notifications are sent.
Destination Type	The type of the destination. Example: SOAP_XML.
Destination Status	Status of the destination device. The status is either Up or Down.
Last Sent	The date and time at which the last notification was sent to the destination device.
Last Failed	The date and time at which the notification had failed.
Total Count	The total count of notifications sent to the destination. Click the count link to view the notification statistics details of the destination device.

Location Template for Controllers

You can define a location template for the controller that you can download to multiple controllers.

You can set the following general and advanced parameters on the location template.

- General parameters—Enable RFID tag collection, set the location path loss for calibrating or normal (non-calibrating) clients, measurement notification for clients, tags, and rogue access points, set the RSSI expiry timeout value for clients, tags, and rogue access points.
- Advanced parameters—Set the RFID tag data timeout value and enable the location path loss configuration for calibrating client multi-band.

Configuring a New Location Template for a Controller

To configure a new location template for a controller, follow these steps:

-
- Step 1** Choose **Configure > Controller Template Launch Pad**.
 - Step 2** Select the **New** (Location Configuration) link under the Location heading to create a new location template (see [Figure 9-2](#)).

Figure 9-2 *Configure > Controller Template Launch Pad Page*

Step 3 In the New Controller Template page, enter a name for the location template on the General tab.

Step 4 On the General tab, modify parameters as necessary. [Table 9-7](#) lists each of the fields.

Table 9-7 *General Tab Fields*

Parameter	Configuration Options
RFID Tag Data Collection	Select the Enabled check box to collect data on tags.
Location Path Loss Configuration	
Calibrating Client	Select the Enabled check box to have a calibrating client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrating clients. Packets are transmitted on all channels. All access points irrespective of channel (and without a channel change) gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic. To use all radios (802.11a/b/g/n) available, you must enable multiband in the Advanced tab.
Normal Client	Select the Enabled check box to have a non-calibrating client. No S36 or S60 requests are transmitted to the client.
Measurement Notification Interval	
Tags, Clients and Rogue APs/Clients	Enter a value to set the Network Mobility Services Protocol (NMSP) measurement notification interval for clients, tags, and rogue access points and clients. This value can be applied to selected controllers through the template. Setting this value on the controller generates out-of-sync notification which you can view in the Services > Synchronize Services page. When a controller and the mobility services engine have two different measurement intervals, the largest interval setting of the two is adopted by the mobility services engine. Once this controller is synchronized with the mobility services engine, the new value is set on the mobility services engine.
RSSI Expiry Timeout	
RSSI Expiry Timeout for Clients	Enter a value to set the RSSI timeout value for normal (non-calibrating) clients.
RSSI Expiry Timeout for Calibrating Clients	Enter a value to set the RSSI timeout value for calibrating clients.

276097

Table 9-7 General Tab Fields (continued)

Parameter	Configuration Options
RSSI Expiry Timeout for Tags	Enter a value to set the RSSI timeout value for tags.
RSSI Expiry Timeout for Rogue APs	Enter a value to set the RSSI timeout value for rogue access points.

Step 5 On the Advanced tab, modify parameters as necessary.

[Table 9-8](#) describes each of the Advanced tab fields.

Table 9-8 Advanced Location Fields

Field	Configuration Options
RFID Tag Data Timeout	Enter an RFID tag data timeout value.
Location Path Loss Configuration	
Calibrating Client Multiband	Select the Enabled check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled on the General tab.

Step 6 Click **Save**.

Location Services on Wired Switches and Wired Clients

You can import the location of wired Catalyst stackable switches (2960, IE-3000, 3560, 3750, 3750-E, switches), switch blades (3020, 3030, 3040, 3110, 3120, 3130), and switch ports into the mobility services engine.

Once you define a wired switch and synchronize it with a mobility services engine, details on wired clients connected to a wired switch are downloaded to the mobility services engine over the NMSP connection. You can then view wired switches and wired clients using the Prime Infrastructure.

Import and display of civic and emergency location identification number (ELIN) meets specifications of RFC 4776, which is outlined at the following URL: <http://tools.ietf.org/html/rfc4776#section-3.4>

This section contains the following topics:

- [Prerequisites to Support Location Services for Wired Clients, page 9-41](#)
- [Guidelines and Limitations, page 9-41](#)
- [Configuring a Catalyst Switch Using the CLI, page 9-41](#)
- [Adding a Catalyst Switch to the Prime Infrastructure, page 9-43](#)
- [Assigning and Synchronizing a Catalyst Switch to a Mobility Services Engine, page 9-43](#)

Prerequisites to Support Location Services for Wired Clients

To support location services for wired clients and wired Catalyst switches, you must do the following:

- Configure the Catalyst switch.
- Add the Catalyst switch to the Prime Infrastructure.
- Catalyst stackable switches and switch blades must be running Cisco IOS Release 12.2(52) SG or later.
- Assign the Catalyst switch to the mobility services engine and synchronize.

Guidelines and Limitations

The following Catalyst 4000 series switches are also supported:

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

Configuring a Catalyst Switch Using the CLI

To configure location services on a wired switch or wired client, and apply it to an interface, follow these steps:



Note All commands are located in the privileged EXEC mode of the command-line interface.

Step 1 Log in to the command-line interface of the switch:

```
Switch > en  
Switch#  
Switch# Configure terminal
```

Step 2 Enable NMSP:

```
Switch(Config)# nmosp  
Switch(config-nmosp)# enable
```

Step 3 Configure the SNMP community:

```
Switch(config)# snmp-server community wired-location
```

Step 4 Enable IP device tracking in the switch:

```
Switch(config)# ip device tracking
```

Step 5 (Optional) Configure a civic location for a switch.



Note You can define a civic and emergency location identification number (ELIN) for a specific location. That identifier can then be assigned to a switch or multiple ports on a switch to represent that location. This location identifier is represented by a single number such as 6 (range 1 to 4095). This saves time when you are configuring multiple switches or ports that reside in the same location.

Enter configuration commands, one per line. End by pressing **Ctrl-Z**.

The following is an example of a civic location configuration:

```
Switch(config)# location civic-location identifier 6
Switch(config-civic)# name "switch-loc4"
Switch(config-civic)# seat "ws-3"
Switch(config-civic)# additional code "1e3f0034c092"
Switch(config-civic)# building "SJ-14"
Switch(config-civic)# floor "4"
Switch(config-civic)# street-group "Cisco Way"
Switch(config-civic)# number "3625"
Switch(config-civic)# type-of-place "Lab"
Switch(config-civic)# postal-community-name "Cisco Systems, Inc."
Switch(config-civic)# postal-code "95134"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state "CA"
Switch(config-civic)# country "US"
Switch(config-civic)# end
```

Step 6 Configure the ELIN location for the switch.



Note The ELIN location length must be between 10 and 25 characters. In the following example, 4084084000 meets that specification. This number can also be entered as 408-408-4000. Additionally, a value with a mix of numerals and text can be entered such as 800-CISCO-WAY or 800CISCOWAY. However, if you place spaces between the numerals or text without hyphens, quotes should be used, such as "800 CISCO WAY."

```
Switch(config)# location elin-location "4084084000" identifier 6
Switch(config)# end
```

Step 7 Configure the location for a port on the switch.

A switch has a specified number of switch ports, and clients and hosts are connected at these ports. When configuring location for a specific switch port, the client connected at that port is assumed to have the port location.

If a switch (switch2) is connected to a port (such as port1) on another switch (switch1) all the clients connected to switch2 are assigned the location that is configured on port1.

The syntax for defining the port is: **interface {GigabitEthernet | FastEthernet} slot/module/port**

Enter only one location definition on a line, and end the line by pressing **Ctrl-Z**.

```
Switch(config)# interface GigabitEthernet 1/0/10
Switch(config-if)# location civic-location-id 6
Switch(config-if)# location elin-location-id 6
Switch(config-if)# end
```

Step 8 Assign a location to the switch itself.

The following port location is configured on the FastEthernet network management port of the switch.

Enter configuration commands, one per line. End by pressing **Ctrl-Z**.

```
Switch(config)# interface FastEthernet 0
Switch(config-if)# location civic-location-id 6
Switch(config-if)# location elin-location-id 6
Switch(config-if)# end
```

Adding a Catalyst Switch to the Prime Infrastructure

All Catalyst switches must be configured with location service before they are added to the Prime Infrastructure. See the [“Configuring a Catalyst Switch Using the CLI”](#) section on page 9-41 for more information.

To add a Catalyst switch configured for wired location service to Prime Infrastructure, follow these steps:

-
- Step 1** Choose **Configure > Switches**.
 - Step 2** From the Select a command drop-down list, choose **Add Switches**. The Add Switches page appears.
 - Step 3** Choose **Device Info** or **File** from the Add Format Type drop-down list.



Note Choose **Device Info** to manually enter one or more switch IP addresses. Choose **File** to import a file with multiple Catalyst switch IP addresses defined. When File is selected, a dialog box appears that defines the accepted format for the imported file.

- Step 4** Enter one or more IP addresses.
- Step 5** From the License Level drop-down list, choose the level of license.
- Step 6** From the Version drop-down list, choose the SNMP version if it is different from the default.
- Step 7** No changes are required in the Retries and SNMP Timeout text boxes.
- Step 8** Enter wired-location as the SNMP community string in the Community text box.



Note The SNMP community string entered at this step must match that value assigned to the Catalyst switch in [Step 3](#) of the [“Configuring a Catalyst Switch Using the CLI”](#) section on page 9-41.

- Step 9** Click **Add**. A page confirming the successful addition to the Prime Infrastructure appears.
 - Step 10** Click **OK** in the Add Switches Result page. The newly added switch appears in the Ethernet Switches page.
-

Assigning and Synchronizing a Catalyst Switch to a Mobility Services Engine

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

All information on wired switches and wired clients connected to those switches downloads to the mobility services engine.



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

To assign and synchronize Catalyst switches to a mobility services engine, follow these steps:

-
- Step 1** Choose **Services > Synchronize Services**.
 - Step 2** Click the **Wired Switches** tab to assign a switch to a mobility services engine.
 - Step 3** Choose one or more switches to be synchronized with the mobility services engine.
 - Step 4** Click **Change MSE Assignment**.
 - Step 5** Choose the mobility services engine to which the switches are to be synchronized.
 - Step 6** 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.
 - Step 7** To verify the NMSP connection between the switch and a mobility services engine, see the [“Verifying an NMSP Connection to a Mobility Services Engine”](#) section on page 9-44.



Note See [Chapter 11, “Monitoring the System and Services”](#) for information on monitoring wired switches.

Verifying an NMSP Connection to a Mobility Services Engine

NMSP manages communication between the mobility services engine and a controller or a location-capable Catalyst switch. Transport of telemetry, emergency, and chokepoint information between the mobility services engine and the controller or location-capable Catalyst switch is managed by this protocol.

To verify an NMSP connection between a mobility services engine and a controller or a location-capable Catalyst switch, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**.
 - Step 2** In the Mobility Services page, click the device name link of the appropriate Catalyst switch or controller.
 - Step 3** Choose **System > Status > NMSP Connection Status**.
 - Step 4** Verify that the NMSP Status is ACTIVE.

If not active, resynchronize the Catalyst switch or controller and the mobility services engine.

**Note**

On a Catalyst wired switch, enter the **show nmsp status** command to verify NMSP connection.



CHAPTER 10

Working with Maps

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

This chapter contains the following sections:

- [About Maps, page 10-1](#)
- [Adding a Campus Map, page 10-2](#)
- [Adding a Building to a Campus Map, page 10-2](#)
- [Adding Floor Areas, page 10-5](#)
- [Monitoring the Floor Area, page 10-10](#)
- [Using the Automatic Hierarchy to Create Maps, page 10-15](#)
- [Using the Map Editor, page 10-17](#)
- [Adding an Outdoor Area, page 10-24](#)
- [Using Planning Mode, page 10-25](#)
- [Using Chokepoints to Enhance Tag Location Reporting, page 10-25](#)
- [Configuring Wi-Fi TDOA Receivers, page 10-29](#)

About Maps

In addition to the features of the legacy maps, the 7.3 Release enables you to use the features of the Next Generation Maps. The Next Generation Maps feature is enabled by default. Use the Administration > User Preferences page to enable or disable this feature.

The Next Generation Maps feature provides you the following benefits:

- Displays large amount of information on the map. When you have various clients, interferers, and access points, they may clutter the display on the Prime Infrastructure map pages and sometimes pages load slowly. The Release 7.3 introduces clustering and layering of information. Information cluster reduces clutter at the high level and reveals more information when you click an object. For details, see the [“Monitoring the Floor Area” section on page 10-10](#).
- Simplifies and accelerates the process of adding APs to the map. In the legacy maps, the process of adding access points to maps was manual and tedious. With Release 7.3, you can use the automated hierarchy creation to add and name the access points. For details, see the [“Using the Automatic Hierarchy to Create Maps” section on page 10-15](#).

- Provides high quality map images with easy navigation and zoom/pan controls. In the legacy maps, the map image quality was low and the navigating, zooming, and panning was slow. With Release 7.3, you can use the next-generation tile-aware map engine to load maps faster and zoom/pan easily. The Next Generation Maps enables you to load high resolution maps faster and navigate around the map easily. For details, see the [“Panning and Zooming with Next Generation Maps” section on page 10-11](#).

This section contains the following topics:

- [“Adding a Campus Map” section on page 10-2](#)
- [“Adding Floor Areas” section on page 10-5](#)
- [“Using the Map Editor” section on page 10-17](#)

Adding a Campus Map

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

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



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

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

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

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

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

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

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

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



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

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

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

Adding a Building to a Campus Map

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

-
- Step 1** Choose **Design > Site Maps** to display the Maps page.
- Step 2** Click the desired campus. The Site Maps > Campus Name page appears.
- Step 3** From the Select a command drop-down list, choose **New Building**, and click **Go**.
- Step 4** In the Campus Name > New Building page, follow these steps to create a virtual building in which you can organize related floor plan maps:
- Enter the building name.
 - Enter the building contact name.
 - Enter the number of floors and basements.
 - Enter the horizontal position (distance from the corner of the building rectangle to the left edge of the campus map) and the vertical position (distance from the corner of the building rectangle to the top edge of the campus map) in feet.



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

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



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



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

- Click **Place** to put the building on the campus map. The Prime Infrastructure creates a building rectangle scaled to the size of the campus map.
- Click the building rectangle and drag it to the desired position on the campus map.



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

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



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

- Step 5** (Optional) To assign location presence information for the new outdoor area, do the following:
- Choose **Edit Location Presence Info** from the Select a command drop-down list. Click **Go**. The Location Presence page appears.



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

- b. Click the **Civic Address** or **Advanced** tab.
 - Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
 - Advanced identifies the campus with expanded civic information such as neighborhood, city division, country, and postal community name.



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

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

Step 6 Click **Save**.

Adding a Standalone Building

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

- Step 1** Choose **Design > Site Maps** to display the Maps page.
- Step 2** From the Select a command drop-down list, choose **New Building**, and click **Go**.
- Step 3** In the Maps > New Building page, follow these steps to create a virtual building in which you can organize related floor plan maps:
 - a. Enter the building name.
 - b. Enter the building contact name.



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

- c. Enter the number of floors and basements.
- d. Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.



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



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

- e. Click **OK** to save this building to the database.

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

- a. Choose **Location Presence** from the Select a command drop-down list. Click **Go**. The Location Presence page appears.
- b. Click the **Civic** or **Advanced** tab.
- Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
 - Advanced identifies the campus with expanded civic information such as neighborhood, city division, county, and postal community name.



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

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

Step 5 Click **Save**.



Note The standalone buildings are automatically placed in the system campus.

Adding Floor Areas

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

This section contains the following topics:

- [“Adding Floor Areas to a Campus Building” section on page 10-5](#)
- [“Adding Floor Plans to a Standalone Building” section on page 10-8](#)

Adding Floor Areas to a Campus Building

After you add a building to a campus map, you can add individual floor plan and basement maps to the building.



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

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

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



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



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



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

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

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

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



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

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

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

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

- a. Enter the floor area and contact names.
- b. Choose the floor or basement number from the Floor drop-down list.
- c. Choose the floor or basement type (RF Model).
- d. Enter the floor-to-floor height in feet.



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

- e. Select the **Image or CAD File** check box.
- f. Browse to and choose the desired floor or basement image or CAD filename, and click **Open**.



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



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

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



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

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



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



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



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

- h. If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.
Enter the remaining parameters for the floor area
- i. Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.
- j. Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.



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

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



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

- l. If desired, select the **Launch Map Editor after floor creation** check box to rescale the floor and draw walls.
- m. Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Design > Site Maps list.



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

Step 8 Click any of the floor or basement images to view the floor plan or basement map.



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

Adding Floor Plans to a Standalone Building

After you have added a standalone building to the Prime Infrastructure database, you can add individual floor plan maps to the building.

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

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



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

Step 2 Browse to and import the floor plan maps from anywhere in your file system. You can import CAD files in DXF or DWG formats or any of the formats you created in Step 1.

**Note**

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

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

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

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

Step 6 Click **Go**.

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

- Enter the floor area and contact names.
- Choose the floor or basement number from the Floor drop-down list.
- Choose the floor or basement type (RF Model).
- Enter the floor-to-floor height in feet.
- Select the **Image or CAD File** check box.
- Browse to and choose the desired floor or basement Image or CAD file, and click **Open**.

**Note**

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

**Tip**

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

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

**Note**

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

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

**Note**

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



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



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

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

Step 9 Enter the remaining parameters for the floor area.

- Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.
- Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.



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

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



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

- Adjust the floor characteristics with the Prime Infrastructure map editor by selecting the check box next to Launch Map Editor. See the [“Using the Map Editor” section on page 10-17](#) for more information regarding the map editor feature.

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

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



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

Monitoring the Floor Area

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

This section contains the following topics:

- [Panning and Zooming with Next Generation Maps, page 10-11](#)

- [Adding Access Points to a Floor Area](#), page 10-11
- [Placing Access Points](#), page 10-14

Panning and Zooming with Next Generation Maps

Panning

To move the map click and hold the left mouse button and drag the map to a new place.

You can also move the map North, South, East, or West using the pan arrows. These can be found on the top left-hand corner of the map (see [Figure 10-1](#)).

Figure 10-1 Panning Control



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

Zooming in and out - changing the scale

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

To see a map with more detail you need to zoom in. You can do this using the zoom bar on the left hand side of the map (see [Figure 10-2](#)). Click the + sign on the top of the zoom bar. To centre and zoom in on a location, double-click the location. To see a map with less detail you need to zoom out. To do this, click the - sign on the bottom of the zoom bar.

Figure 10-2 Zooming Control



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

Adding Access Points to a Floor Area

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

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

- Step 2** From the Maps Tree View or the Design > Site Maps left sidebar menu, choose the applicable floor to open the Floor View page.
- Step 3** From the Select a command drop-down list, choose **Add Access Points**, and click **Go**.
- Step 4** In the Add Access Points page, select the check boxes of the access points that you want to add to the floor area.



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



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



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

- Step 5** When all of the applicable access points are selected, click **OK** located at the bottom of the access point list.

The Position Access Points page appears.

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

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



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



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

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

- AP Model—Indicates the model type of the selected access point.
- Protocol—Choose the protocol for this access point from the drop-down list.
- Antenna—Choose the appropriate antenna type for this access point from the drop-down list.
- Antenna/AP Image—The antenna image reflects the antenna selected from the Antenna drop-down list. Click the arrow at the top right of the antenna image to expand the image size.
- Antenna Orientation—Depending on the antenna type, enter the Azimuth and the Elevation orientations in degrees.



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



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

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

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



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

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

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



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

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



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



Note Antenna gain settings have no effect on heatmaps and location calculations. Antenna gain is implicitly associated to the antenna name. Because of this, the following apply:

- If an antenna is used and marked as “Other” in the Prime Infrastructure, it is ignored for all heatmap and location calculations;
- If an antenna is used and marked as a Cisco antenna in the Prime Infrastructure, that antenna gain setting (internal value on the Prime Infrastructure) is used no matter what gain is set on the controller.



Note See the “[Placing Access Points](#)” section on page 10-14 for more information on placing access points on a map.



Note You can change the position of access points by importing or exporting a file. See the [“Positioning Wi-Fi TDOA Receivers” section on page 10-31](#) for more information.

Placing Access Points

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

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

1. Most importantly, access points should surround the desired location.
2. One access point should be placed roughly every 50 to 70 linear feet (about 17 to 20 meters). This translates into one access point every 2,500 to 5000 square feet (about 230 to 450 square meters).



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

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



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



Note If you have a ceiling-mounted AP with an integrated omni-directional antenna, the antenna orientation does not really need to be set in the Prime Infrastructure. However, if you mount that same AP on the wall, you must set the antenna orientation to 90 degrees.

[Table 10-1](#) describes the orientation of the access points.

Table 10-1 *Antenna Orientation of the Access Points*

Access Point	Antenna Orientation
1140 mounted on the ceiling	The Cisco logo should be pointing to the floor. Elevation: 0 degrees.

Table 10-1 Antenna Orientation of the Access Points (continued)

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

Using the Automatic Hierarchy to Create Maps

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

**Note**

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

- Step 1** Choose **Design > Automatic Hierarchy Creation** to display the Automatic Hierarchy Creation page.
- Step 2** In the text box, enter the name of an access point on your system. Or, you can choose one from the list. This name is used to create a regular expression to create your maps.

**Note**

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

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

- Step 3** Click **Next**.
- Step 4** If your access point's name has a delimiter, enter it in the text box and click **Generate**. The system generates a regular expression that matches your access point's name based on the delimiter. For example, using the dash (-) delimiter in the access point name San Jose-01-GroundFloor-AP3500i1, produces the regular expression `/(.*)-(.*)-(.*)-(.*)/`. If you have a more complicated access point name, you can manually enter the regular expression.



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

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

Step 6 Using the Group fields, assign matching groups to hierarchy types.

For example, if your access point is named: SJC14-4-AP-BREAK-ROOM

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

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

From the AP name, the following groups are extracted:

1. SJC
2. 14
3. 4
4. AP-BREAK-ROOM

The matching groups are assigned from left to right, starting at 1.

To make the matching groups match the hierarchy elements, use the drop-down list for each group number to select the appropriate hierarchy element.

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

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

If you use the regular expression: `/(.*)-(.*)-(.*)-(.*)/`

with the following group mapping:

1. Building
2. Device Name
3. Floor
4. Campus

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



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

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

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

Yes	No	No	Failed match
No	Yes	Yes	System Campus > Building > Floor
No	Yes	No	Failed match
No	No	Yes	Failed match
No	No	No	Failed match

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

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

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

Step 7 Click **Next**. You can test against more access points. You may test your regular expression and matching group mapping against more access points by entering the access point's names in the Add more device names to test against field, and clicking the **Add** button.

You then click the **Test** button to test each of the access points names in the table. The result of each test is displayed in the table.

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

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



Note

You can edit the maps to include floor images, correct dimensions, and so on. When Automatic Hierarchy Creation creates a map, it uses the default dimensions of 20 feet by 20 feet. You will need to edit the created maps to specify the correct dimensions and other attributes.

Maps created using Automatic Hierarchy Creation appear in the maps list with an *incomplete* icon. Once you have edited a map, the *incomplete* icon disappears. You may hide the column for incomplete maps by clicking the Edit View link.

Using the Map Editor

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

Guidelines for Using the Map Editor

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

- We recommend that you use the map editor to draw walls and other obstacles rather than importing an .FPE file from the legacy floor plan editor.
 - If necessary, you can still import .FPE files. To do so, navigate to the desired floor area, choose **Edit Floor Area** from the Select a command drop-down list, click **Go**, select the **FPE File** check box, and browse to choose the .FPE file.
- You can add any number of walls to a floor plan with the map editor; however, the processing power and memory of a client workstation might limit the refresh and rendering aspects of the Prime Infrastructure.
 - We recommend a practical limit of 400 walls per floor for machines with 1GB RAM or less.
- All walls are used by the Prime Infrastructure when generating RF coverage heatmaps.

Guidelines for Inclusion and Exclusion Areas on a Floor

Inclusion and exclusion areas can be any polygon shape and must have at least three points.

You can only define one inclusion region on a floor. By default, an inclusion region is defined for each floor when it is added to the Prime Infrastructure. The inclusion region is indicated by a solid aqua line, and generally outlines the region.

You can define multiple exclusion regions on a floor.

Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

Opening the Map Editor

Follow these steps to use the map editor:

-
- Step 1** Choose **Design > Site Map Design**.
 - Step 2** Click the desired campus. The Site Maps > Campus Name page appears.
 - Step 3** Click a campus and then click a building.
 - Step 4** Click the desired floor area. The Site Maps > Campus Name > Building Name > Floor Area Name page appears.
 - Step 5** From the Select a command drop-down list, choose **Map Editor**, and click **Go**. The Map Editor page appears.
-

Map Editor Icons

Table 10-2 Next Generation Maps Icons

Icon	Description
	Scale Floor—Click anywhere on the map to start drawing line. Double-click to finish the line and enter the new line length in the pop up shown. This will modify the floor dimensions to the new dimensions.
	Measure Distance—Click anywhere on the map to start drawing line. Double-click to finish the line. Measured line length in ft/meters is shown on the top.
	Copy/Move Obstacles—Select obstacles either by drawing a box on the map or by clicking on the obstacles. To copy obstacles, click the 'Copy' button. This will create new obstacles just above the selected obstacles. To move the obstacles, drag the selected obstacles to new position. Clicking anywhere on the map will unselect all the elements.
	Delete Mode—Select the elements to be deleted either by drawing a box on the map or clicking on each element. Use Shift key to select multiple elements. Use the Ctrl key to toggle selection of elements, one at a time. Clicking anywhere on the map will unselect all the elements. Click the 'Delete' button to delete the selected elements
	Modify Mode—Click an element and click the vertices to reshape or drag the element to move to a new position. Clicking anywhere on the map will unselect the selected element.
	Draw Coverage Area
	Draw Location Region
	Draw Rail
	Draw Obstacle—Click anywhere on the map to start drawing. Double-click to finish drawing. Use Ctrl-z to undo, Ctrl-y to redo, and, the 'Esc' key to cancel the current drawing.
	Place Marker
	Navigation—Remove any selected modes such as drawing or editing and switches to navigation mode where you can view the map and perform zooming or panning.

Using the Map Editor to Draw Coverage Areas

If you have a building that is non-rectangular or you want to mark a non-rectangular area within a floor, you can use the map editor to draw a coverage area.

-
- Step 1** Add the floor plan if it is not already represented in the Prime Infrastructure.
- Step 2** Choose **Design > Site Maps**.

- Step 3** Click the Map Name that corresponds to the outdoor area, campus, building, or floor you want to edit.
- Step 4** From the Select a command drop-down list, choose **Map Editor**, and click **Go**.
- Step 5** In the Map Editor page, click the **Draw Coverage Area** icon on the toolbar.
A pop-up appears.
- Step 6** Enter the name of the area that you are defining. Click **OK**.
A drawing tool appears.
- Step 7** Move the drawing tool to the area you want to outline.
- Click the left mouse button to begin and end drawing a line.
 - When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page.
- The outlined area must be a closed object to appear highlighted on the map.
- Step 8** Click the disk icon on the toolbar to save the newly drawn area.

Using the Map Editor to Draw Obstacles

Table 10-3 describes the obstacle color coding.

Table 10-3 Obstacle Color Coding

Type of obstacle	Color coding	Loss (in dB)
Thick wall		13
Light wall		2
Heavy door		15
Light door		4
Cubicle		1
Glass		1.5

Map Editor Edit Mode

In the Next generation map editor, you can edit the area using the Edit Mode option available. In the legacy maps, if you have made a mistake in drawing, then you have to delete it and redraw again. But in the Next generation map editor, you can choose Edit Mode and click on the area to be edited and drag the vertices or hold down the mouse key and move the entire area to a different place.

Defining an Inclusion Region on a Floor

To define an inclusion area, follow these steps:

- Step 1** Choose **Design > Site Maps**.
- Step 2** Click the name of the appropriate floor area.
- Step 3** From the Select a command drop-down list, choose **Map Editor**.
- Step 4** Click **Go**.
- Step 5** At the map, click the aqua box on the toolbar.



Note A message box appears reminding you that only one inclusion area can be defined at a time. Defining a new inclusion region automatically removes the previously defined inclusion region. By default, an inclusion region is defined for each floor when it is added to the Prime Infrastructure. The inclusion region is indicated by a solid aqua line and generally outlines the region.

- Step 6** Click **OK** in the message box that appears. A drawing icon appears to outline the inclusion area.
- Step 7** To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.
- Step 8** Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.
- Step 9** Repeat [Step 8](#) until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area.
- Step 10** Choose **Save** from the Command menu or click the **disk** icon on the toolbar to save the inclusion region.



Note If you made an error in defining the inclusion area, click the area. The selected area is outlined by a dashed aqua line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.

- Step 11** Select the **Location Regions** check box if it is not already selected. If you want it to apply to all floor maps, click **Save settings**. Close the Layers configuration page.
- Step 12** To resynchronize the Prime Infrastructure and MSE databases, choose **Services > Synchronize Services**.



Note If the two DBs are already synchronized then a resynchronization happens automatically every time there is a change. There is no need for an explicit resynch.

- Step 13** In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.



Note Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

Defining an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are generally defined within the borders of an inclusion area.

To define an exclusion area, follow these steps:

-
- Step 1** Choose **Design > Site Maps**.
 - Step 2** Click the name of the appropriate floor area.
 - Step 3** From the Select a command drop-down list, choose **Map Editor**.
 - Step 4** Click **Go**.
 - Step 5** At the map, click the purple box on the toolbar.
 - Step 6** Click **OK** in the message box that appears. A drawing icon appears to outline the exclusion area.
 - Step 7** To begin defining the exclusion area, move the drawing icon to the starting point on the map, and click once.
 - Step 8** Move the drawing icon along the boundary of the area you want to exclude. Click once to start a boundary line, and click again to end the boundary line.
 - Step 9** Repeat [Step 8](#) until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is completely defined. The excluded area is shaded in purple.
 - Step 10** To define additional exclusion regions, repeat [Step 5](#) to [Step 9](#).
 - Step 11** When all exclusion areas are defined, choose **Save** from the Command menu or click the **disk** icon on the toolbar to save the exclusion region.



Note To delete an exclusion area, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.

- Step 12** Select the **Location Regions** check box if it is not already selected, click **Save settings**, and close the Layers configuration page when complete.
- Step 13** To resynchronize the Prime Infrastructure and location databases, choose **Services > Synchronize Services**.
- Step 14** In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Defining a Rail Line on a Floor

You can define a rail line on a floor that represents a conveyor belt. Additionally, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority).



Note Rail line configurations do not apply to tags.

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

To define a rail with a floor, follow these steps:

-
- Step 1** Choose **Design > Site Maps**.
 - Step 2** Click the name of the appropriate floor area.
 - Step 3** Choose **Map Editor** from the Select a command drop-down list.
 - Step 4** Click **Go**.
 - Step 5** In the map, click the **rail** icon (to the right of the purple exclusion icon) on the toolbar.
 - Step 6** In the message dialog box that appears, enter a snap-width (feet or meters) for the rail and then click **OK**. A drawing icon appears.
 - Step 7** Click the **drawing** icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.
 - Step 8** Click the **drawing** icon twice when the rail line is completely drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.



Note To delete a rail line, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the X icon on the toolbar. The area is removed from the floor map.

- Step 9** At the floor map, choose the **Layers** drop-down list.
- Step 10** Select the **Rails** check box for if it is not already selected, click **Save settings**, and close the Layers configuration panel when complete.
- Step 11** To resynchronize the Prime Infrastructure and mobility services engine, choose **Services > Synchronize Services**.
- Step 12** In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Adding an Outdoor Area


Note

You can add an outdoor area to a campus map in the Prime Infrastructure database regardless of whether you have added outdoor area maps to the database.

To add an outdoor area to a campus map, follow these steps:

- Step 1** If you want to add a map of the outdoor area to the database, save the map in .PNG, .JPG, .JPEG, or .GIF format. Then browse to and import the map from anywhere in your file system.


Note

You do not need a map to add an outdoor area. You can simply define the dimensions of the area to add it to the database. The map can be any size because the Prime Infrastructure automatically resizes the map to fit the workspace.

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

- Step 3** Click the desired campus to display the Design > Site Maps > Campus View page.

- Step 4** From the Select a command drop-down list, choose **New Outdoor Area**.

- Step 5** Click **Go**. The Create New Area page appears.

- Step 6** In the New Outdoor Area page, enter the following information:

- Name—The user-defined name of the new outdoor area.
- Contact—The user-defined contact name.
- Area Type (RF Model)—Cubes And Walled Offices, Drywall Office Only, Outdoor Open Space (default).
- AP Height (feet)—Enter the height of the access point.
- Image File—Name of the file containing the outdoor area map. Click **Browse** to find the file.

- Step 7** Click **Next**.

- Step 8** Click **Place** to put the outdoor area on the campus map. the Prime Infrastructure creates an outdoor area rectangle scaled to the size of the campus map.

- Step 9** Click and drag the outdoor area rectangle to the desired position on the campus map.

- Step 10** Click **Save** to save this outdoor area and its campus location to the database.


Note

A hyperlink associated with the outdoor area takes you to the corresponding Maps page.

- Step 11** (Optional) To assign location presence information for the new outdoor area, choose **Edit Location Presence Info**, and click **Go**.


Note

By default, the Override Child Element Presence Info check box is selected. There is no need to alter this setting for outdoor areas.

Using Planning Mode

The planning mode opens the map editor in the browser window from which the planning tool is launched. If the original browser window has navigated away from the floor page, you need to navigate back to the floor page to launch the map editor.

You can calculate the recommended number and location of access points based on whether data and/or voice traffic and/or location are active.

**Note**

Based on the throughput specified for each protocol (802.11a or 802.11 b/g), planning mode calculates the total number of access points required that would provide optimum coverage in your network.

Planning Mode options:

- Add APs—Enables you to add access points on a map. See the [“Adding Access Points to a Floor Area” section on page 10-11](#) for details.
- Delete APs—Deletes the selected access points.
- Map Editor—Opens the Map Editor window. See the [“Using the Map Editor” section on page 10-17](#) for more details.
- Synchronize with Deployment—Synchronizes your planning mode access points with the current deployment scenario.
- Generate Proposal—View a planning summary of the current access points deployment.
- Planned AP Association Tool—Allows you to perform add, delete or import an AP Association from an excel or CSV file. Once an access point is defined, it can be associated to a base radio MAC address using the Planned AP Association Tool. If the AP is not discovered they get pushed into a standby bucket and get associated when discovered.

**Note**

AP association is subjected to a limitation that AP should not belong to any floor or outdoor area. If the AP is already assigned to a floor or outdoor area, then the standby bucket holds the AP and when removed from the floor or outdoor, get positioned to the given floor. One Mac address cannot be put into bucket for multiple floor or outdoor areas.

**Note**

The map synchronizations works only if the AP is associated to a base radio MAC address and not to its Ethernet MAC address.

Using Chokepoints to Enhance Tag Location Reporting

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be entered into the location database and plotted on the Prime Infrastructure map.

Using chokepoints in conjunction with active Cisco CX compliant tags provides immediate location information on a tag and its asset. When a Cisco CX tag moves out of the range of a chokepoint, its subsequent beacon frames do not contain any identifying chokepoint information. Location determination of the tag defaults to the standard calculation methods based on RSSIs reported by access point associated with the tag.

**Note**

See the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide* for chokepoint installation, configuration, and management details at the following URL: <http://support.aeroscout.com>

This section contains the following topics:

- [Guidelines and Limitations, page 10-26](#)
- [Adding Chokepoints to the Prime Infrastructure, page 10-26](#)
- [Removing Chokepoints from the Prime Infrastructure, page 10-29](#)

Guidelines and Limitations

- The chokepoint range is product-specific and is supplied by the chokepoint vendor.
- You generally enable a chokepoint that is placed near an exit to function as an entry/exit (perimeter) chokepoint. When a client or tag shows strong RSSIs on two floors, you can check for the last perimeter chokepoint that the tag or client passed to determine the current floor location of that client or tag.
- The rings around the chokepoint icon indicate the coverage area. When a Cisco CX tag and its asset pass within the coverage area, location details are broadcast and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and it is no longer mapped on the chokepoint rings.

Adding Chokepoints to the Prime Infrastructure

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

-
- Step 1** Choose **Configure > Chokepoints**.
 - Step 2** From the Select a command drop-down list, choose **Add Chokepoints**.
 - Step 3** Click **Go**.
 - Step 4** Enter the MAC address and name for the chokepoint.
 - Step 5** Select the **Entry/Exit Chokepoint** check box.
 - Step 6** Enter the coverage range for the chokepoint.

**Note**

The Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

- Step 7** Click **OK**.



Note After the chokepoint is added to the database, it can be placed on the appropriate the Prime Infrastructure floor map.

Adding a Chokepoint to a Prime Infrastructure Map

To add the chokepoint to a map, follow these steps:

-
- Step 1** Choose **Design > Site Maps**.
 - Step 2** In the Maps page, choose the link that corresponds to the floor location of the chokepoint.
 - Step 3** From the Select a command drop-down list, choose **Add Chokepoints**.
 - Step 4** Click **Go**.



Note The Add Chokepoints summary page lists all recently added chokepoints that are in the database but are not yet mapped.

- Step 5** Select the check box next to the chokepoint that you want to place on the map.
- Step 6** Click **OK**.

A map appears with a chokepoint icon located in the top left-hand corner. You are now ready to place the chokepoint on the map.

- Step 7** Left-click the chokepoint icon and drag it to the proper location.



Note The MAC address, name, and coverage range of the chokepoint appear in the dialog box in the left when you click the chokepoint icon for placement.

- Step 8** Click **Save**.

You are returned to the floor map and the added chokepoint appears on the map.



Note The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.



Note The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.



Note The MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint appear when you hover your mouse cursor over its map icon.

- Step 9** If the chokepoint does not appear on the map, select the **Chokepoints** check box located in the Floor Settings menu.



Note Do not click **Save Settings** unless you want to save this display criteria for all maps.



Note You must synchronize network design to the mobility services engine or location server to push chokepoint information.

Positioning Chokepoints

To position chokepoints on the map, follow these steps:

- Step 1** Left-click the **Chokepoint** icon and drag it to the proper location.



Note The MAC address, name, and coverage range of the chokepoint appear in the dialog box in the left when you click the chokepoint icon for placement.

- Step 2** Click **Save** when the icon is correctly placed on the map.

- Step 3** The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.



Note The rings around the chokepoint icon indicate the coverage area. When a Cisco Compatible Extensions tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. The chokepoint range is provided as a visual only, but chokepoint vendor software is required to actually configure the range. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.



Note The MAC address, name, and range of a chokepoint are displayed when you hover your mouse cursor over its map icon.

- Step 4** If the chokepoint does not appear on the map, choose **Layers** to view a drop-down list of possible elements to display on the map. Select the **Chokepoints** check box.



Note Do not click **Save Settings** unless you want to save this display criteria for all maps.



Note You can change the position of chokepoints by importing or exporting a file.

Removing Chokepoints from the Prime Infrastructure

You can remove one or more chokepoints at a time.

To delete a chokepoint, follow these steps:

-
- Step 1** Choose **Configure > Chokepoints**. The Chokepoints page appears.
 - Step 2** Select the check box next to the chokepoint to be deleted.
 - Step 3** From the Select a command drop-down list, choose **Remove Chokepoints**, and click **Go**.
 - Step 4** To confirm the chokepoint deletion, click **OK** in the dialog box that appears.
- The Chokepoints page reappears and confirms the deletion of the chokepoints. The deleted chokepoints are no longer listed in the page.
-

Configuring Wi-Fi TDOA Receivers

The Wi-Fi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine for used in calculating the location of a tagged asset. TDOA receivers use the Time Difference of Arrival (TDOA) method to calculate tag location. TDOA uses data from a minimum of three TDOA receivers to generate the location of a tagged asset.

**Note**

If a TDOA receiver is not in use, then the location calculations for tags are generated using RSSI readings from access points.

This section contains the following topics:

- [Prerequisites for Using TDOA Receiver Within the Cisco Unified Wireless Network, page 10-29](#)
- [Adding Wi-Fi TDOA Receivers to the Prime Infrastructure Database, page 10-30](#)
- [Adding Wi-Fi TDOA Receivers to a Map, page 10-30](#)
- [Positioning Wi-Fi TDOA Receivers, page 10-31](#)
- [Removing Wi-Fi TDOA Receivers from the Prime Infrastructure, page 10-31](#)

Prerequisites for Using TDOA Receiver Within the Cisco Unified Wireless Network

Before using a TDOA receiver within the Cisco Unified Wireless Network, you must do the following:

1. Have a mobility services engine active in the network.
2. Add the TDOA receiver to the Prime Infrastructure database and map.
3. Synchronize the Prime Infrastructure and mobility services engines.
4. Set up the TDOA receiver using the *AeroScout System Manager*.

**Note**

See the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide* for configuration details at the following URL: <http://support.aeroscout.com>.

Adding Wi-Fi TDOA Receivers to the Prime Infrastructure Database

To add Wi-Fi TDOA receivers to the Prime Infrastructure database, follow these steps:

-
- Step 1** Choose **Configure > WiFi TDOA Receivers**.
 - Step 2** From the Select a command drop-down list, choose **Add WiFi TDOA Receivers**.
 - Step 3** Click **Go**.
 - Step 4** Enter the MAC address, name, and static IP address for the Wi-Fi TDOA receiver.

**Note**

Wi-Fi TDOA receivers are configured separately using the Wi-Fi TDOA receiver vendor software.

- Step 5** Click **OK** to save the Wi-Fi TDOA receiver entry to the database.

**Note**

After the Wi-Fi TDOA receiver is added to the database, place it on the appropriate Prime Infrastructure floor map. See the “[Adding Wi-Fi TDOA Receivers to the Prime Infrastructure Database](#)” section on page 10-30 for more information.

Adding Wi-Fi TDOA Receivers to a Map

To add a Wi-Fi TDOA receiver to a map, follow these steps:

-
- Step 1** Choose **Design > Site Maps**.
 - Step 2** Choose the link that corresponds to the floor location of the Wi-Fi TDOA receiver.
 - Step 3** From the Select a command drop-down list, choose **Add WiFi TDOA Receivers**.
 - Step 4** Click **Go**.

**Note**

The Add WiFi TDOA Receivers summary page lists all recently added Wi-Fi TDOA receivers that are in the database but are not yet mapped.

- Step 5** Select the check box next to the Wi-Fi TDOA receiver to be added to the map.
- Step 6** Click **OK**.

A map appears with a green WiFi TDOA receiver icon located in the top left-hand corner. You are now ready to position the Wi-Fi TDOA receiver on the map.

Positioning Wi-Fi TDOA Receivers

To position Wi-Fi TDOA receivers on the map, follow these steps:

Step 1 Left-click the **WiFi TDOA receiver** icon and drag it to the proper location.



Note The MAC address and name of the Wi-Fi TDOA receiver appear in the left pane when you click the WiFi TDOA receiver icon for placement.

Step 2 Click **Save** when the icon is correctly placed on the map.



Note The MAC address of the Wi-Fi TDOA receiver appears when you hover your mouse cursor over its map icon.

Step 3 If the chokepoint does not appear on the map, click **Layers** to view a drop-down list of possible elements to display on the map. Select the **WiFi TDOA Receivers** check box.



Note Do not select **Save Settings** unless you want to save this display criteria for all maps.



Note You can change the position of Wi-Fi TDOA Receivers by importing or exporting a file.

Removing Wi-Fi TDOA Receivers from the Prime Infrastructure

You can remove one or more Wi-Fi TDOA receivers at a time. If you remove a TDOA receiver from a map, it remains in the Prime Infrastructure database but is labeled as unassigned.

To delete a TDOA receiver from Prime Infrastructure, follow these steps:

Step 1 Choose **Configure > WiFi TDOA Receivers**. The WiFi TDOA Receivers summary page appears.

Step 2 Select the check box next to each TDOA receiver to be deleted.

Step 3 From the Select a command drop-down list, choose **Remove WiFi TDOA Receivers**, and click **Go**.

Step 4 To confirm TDOA receiver deletion, click **OK** in the pop-up dialog box that appears.

The All WiFi TDOA Receivers page appears. A message confirming deletion of the TDOA receiver appears. The deleted TDOA receiver is no longer listed in the page.

c



CHAPTER 11

Monitoring the System and Services

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

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

This chapter contains the following sections:

- [Working with Alarms, page 11-1](#)
- [Working with Events, page 11-6](#)
- [Working with Logs, page 11-6](#)
- [Generating Reports, page 11-8](#)
- [Client Support on the MSE, page 11-41](#)

Working with Alarms

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

This section contains the following topics:

- [Guidelines and Limitations, page 11-1](#)
- [Viewing Alarms, page 11-2](#)
- [Viewing the MSE Alarm Details, page 11-2](#)
- [Assigning and Unassigning Alarms, page 11-4](#)
- [Deleting and Clearing Alarms, page 11-5](#)
- [E-mailing Alarm Notifications, page 11-5](#)

Guidelines and Limitations

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

Viewing Alarms

To view mobility services engine alarms, follow these steps:

Step 1 Choose **Monitor > Alarms**.



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

Step 2 Click the **Advanced Search** link in the navigation bar. A configurable search dialog box for alarms appears.

Step 3 Choose **Alarms** from the Search Category drop-down list.

Step 4 Choose the Severity of Alarms from the Severity drop-down list to display. The options are **All Severities**, **Critical**, **Major**, **Minor**, **Warning**, or **Clear**.

Step 5 Choose **Mobility Service** from the Alarm Category drop-down list.

Step 6 Choose the **Condition** from the Condition combo box. Alternatively, you can also enter the condition in the Condition in the combo box.

Step 7 From the Time Period drop-down list, choose the time frame for which you want to review alarms. The options range from minutes (5, 15, and 30) to hours (1 and 8) to days (1 and 7). To display all, choose **Any time**.

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

Step 9 Select the **Assigned State** check box to exclude the assigned alarms and their count in the Alarm Summary page.

Step 10 From the Items per page drop-down list, choose the number of alarms to display in each page.

Step 11 To save the search criteria for later use, select the **Save Search** check box and enter a name for the search.



Note You can initiate the search thereafter by clicking the **Saved Search** link.

Step 12 Click **Go**. The alarms summary dialog box appears with search results.



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

Step 13 Repeat [Step 2](#) to [Step 12](#) to see Context-Aware Service notifications for the mobility services engine. Enter **Context Aware Notifications** as the alarm category in [Step 5](#).

Viewing the MSE Alarm Details

To view MSE alarm details, follow these steps:

Step 1 Choose **Monitor > Alarms**.

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

Alternatively, you can choose the **Services > Services > MSE Name > System > Status > Prime Infrastructure Alarms** page and click a particular MSE item in the Failure Source column to access the alarm details for a particular MSE (see [Figure 11-1](#)).

Figure 11-1 MSE Alarm

906182
281906

[Table 11-1](#) lists the various fields in the Alarm Detail page for an MSE.

Table 11-1 General Parameters

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



Note

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

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

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



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

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

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

Select a command

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

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



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

- Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.
- Unacknowledge—You can choose to unacknowledge an already acknowledged alarm.
- Email Notification—Opens the All Alarms > Email Notification page to view and configure e-mail notifications.
- Event History—Opens the Monitor > Events page to view events for this alarm.

Assigning and Unassigning Alarms

To assign and unassign an alarms, follow these steps:

- Step 1** Choose **Monitors > Alarms** to display the Alarms page.
- Step 2** Select the alarms that you want to assign to yourself by selecting their corresponding check boxes.



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

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

Deleting and Clearing Alarms

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

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

-
- Step 1** Choose **Monitors > Alarms** to display the Alarms page.
- Step 2** Select the alarms that you want to delete or clear by selecting their corresponding check boxes.
- Step 3** From the Select a command drop-down list, choose **Delete** or **Clear**. Click **Go**.
-

E-mailing Alarm Notifications

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

You can choose the alarm severity types (critical, major, minor, and warning) to have e-mailed to you.

To send alarm notifications, follow these steps:

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



Note An SMTP mail server must be defined before you enter target e-mail addresses for e-mail notification. Choose **Administration > Settings > Mail Server Configuration** to enter the appropriate information.

- Step 3** Select the **Enabled** check box next to the Mobility Service.



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

- Step 4** Click the **Mobility Service** link. The page for configuring the alarm severity types that are reported for the mobility services engine appears.
- Step 5** Select the check box next to all the alarm severity types for which you want e-mail notifications sent.
- Step 6** In the To text box, enter the e-mail address or addresses to which you want the e-mail notifications sent. Separate e-mail addresses by commas.
- Step 7** Click **OK**.

You are returned to the Alarms > Notification page. The changes to the reported alarm severity levels and the recipient e-mail address for e-mail notifications are displayed.

Working with Events

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

Displaying Location Notification Events

To display location notification events, follow these steps:

Step 1 Choose **Monitor > Events**.

Step 2 In the Events page, you can perform the following:

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

Step 3 If the Prime Infrastructure finds events that match the search criteria, it shows a list of these events.



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

Working with Logs

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

This section contains the following topics:

- [Guidelines and Limitations, page 11-6](#)
- [Configuring Logging Options, page 11-7](#)
- [MAC Address-based Logging, page 11-8](#)
- [Downloading Log Files, page 11-8](#)

Guidelines and Limitations

- When you are selecting an appropriate option from the logging level, make sure you use Error and Trace only when directed to do so by Cisco TAC personnel.

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

Configuring Logging Options

You can use the Prime Infrastructure to specify the logging level and types of messages to log. To configure logging options, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the mobility services engine that you want to configure.
- Step 3** From the System menu, choose **Logs**. The logging options for the selected mobility services engine appear.
- Step 4** Choose the appropriate options from the Logging Level drop-down list.

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

All log records with a log level of Error or above are logged to a new error log file `locserver-error-%u-%g.log`. This is an additional log file maintained along with the location server `locserver-%u-%g.log` log file. The error log file consists of logs of Error level along with their context information. The contextual information consists of 25 log records prior to the error. You can maintain up to 10 error log files. The maximum size allowed for each log file is 10 MB.



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

- Step 5** Select the **Enable** check box next to each element listed in that section to begin logging of its events.
- Step 6** Select the **Enable** check box under Advanced Parameters to enable advanced debugging. By default, this option is disabled.



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

- Step 7** To download log files from the server, click **Download Logs**. For more information, see the [“Downloading Log Files” section on page 11-8](#).
- Step 8** In the Log File group box, enter the following:
- The number of log files to be maintained in the mobility services engine. You can maintain a minimum of 5 log files and a maximum of 20 log files in the mobility services engine.
 - The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.
- Step 9** In the MAC Address Based Logging page, do the following:
- Select the **Enable** check box to enable MAC address logging. By default, this option is disabled.
 - Add one or more MAC addresses for which you want to enable logging. You can also remove MAC addresses that you have already added by selecting the MAC address from the list and clicking **Remove**.

For more information on MAC address-based logging, see the [“MAC Address-based Logging” section on page 11-8](#).

Step 10 Click **Save** to apply your changes.

MAC Address-based Logging

This feature allows you to create log files that are specific to an entity whose MAC address is specified. The log files are created in the locserver directory under the following path:

/opt/mse/logs/locserver

A maximum of 5 MAC addresses can be logged at a time. The log file format for MAC address aa:bb:cc:dd:ee:ff is:

macaddress-debug-aa-bb-cc-dd-ee-ff.log

You can create a maximum of two log files for a MAC address. The two log files may consist of one main and one back up or rollover log file.

The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC address. The MAC log files which are not updated for more than 24 hours are pruned.

Downloading Log Files

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

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

- Step 1** Choose **Services > Mobility Services Engines**.
 - Step 2** Click the name of the mobility services engine to view its status.
 - Step 3** From the left sidebar menu, choose **Logs**.
 - Step 4** Click **Download Logs**.
 - Step 5** Follow the instructions in the File Download dialog box to view the file or save the .zip file to your system.
-

Generating Reports

In the Prime Infrastructure, you can generate various kinds of reports. This section explains how to generate ContextAware reports using the Prime Infrastructure Report Launch Pad. By default, reports are stored on the Prime Infrastructure server.

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

You can define the following criteria for the reports:

- Which mobility services engine or engines to monitor
- How often the report is generated
- How the data is graphed on the charts

- Whether the report is e-mailed or exported to a file

This section contains [Report Launch Pad, page 11-9](#)

Report Launch Pad

The report launch pad provides access to all the Prime Infrastructure reports from a single page. In this page, you can view current reports, open specific types of reports, create and save new reports, and manage scheduled runs. You can access the ContextAware reports section in the Report Launch Pad to generate ContextAware reports.



Tip

Hover your mouse cursor over the tool tip next to the report type to view more report details.

This section contains the following topics:

- [Creating and Running a New Report, page 11-9](#)
- [Managing Current Reports, page 11-15](#)
- [Managing Scheduled Run Results, page 11-15](#)
- [Managing Saved Reports, page 11-16](#)

Creating and Running a New Report

To create and run a new report, follow these steps:

Step 1 Choose **Reports > Report Launch Pad**.

The reports are listed by category in the main section of the page and on the left sidebar menu.

Step 2 Find the appropriate report in the main section of the Report Launch Pad.



Note Click the report name from the Report Launch Pad or use the navigation on the left side of the Report Launch Pad page to view any currently saved reports for that report type.

Step 3 Click **New**. The Report Details page appears (see [Figure 11-2](#)).

Figure 11-2 Report Details Page

Busiest Clients : New
 Reports > [Report Launch Pad](#) > Client > [Busiest Clients](#) > **Busiest Clients Report Details**

Save Save and Run Run Now Cancel

Settings	Schedule
Report Title: <input type="text"/>	Scheduling: <input type="checkbox"/> Enable
Report By: Controller	Export Format: CSV
Report Criteria: All Controllers <input type="button" value="Edit"/>	Destination: File C:\WCS-FTP\reports\BusiestClients\<ReportTitleN
Protocol: All Clients	Start Date/Time: 02/17/2009 09:55 Current Server Time: 02/17/2009 09:58:09 PST
Reporting Period: Last 1 Hour	Recurrence: No Recurrence
From: <input type="text"/> :00	
To: <input type="text"/> :00	
Show: Up to 5 records <small>(Leave blank to show all records.)</small>	Customize Report Format Click here to customize report content based on your preference. <input type="button" value="Customize"/>

Report Run Result 251857

Step 4 In the Report Details page, enter the following Settings parameters:



Note Certain parameters may or may not appear depending on the report type.

- Report Title—If you plan to use this as a saved report, enter a report name.
- Report By—Choose the appropriate Report By category from the drop-down list.
- Report Criteria—Allows you to sort your results depending on the previous Report By selection made. Click **Edit** to open the Filter Criteria page.



Note Click **Select** to confirm your filter criteria or **Close** to return to the previous page.

- Connection Protocol—All Clients, All Wired(802.3), All Wireless (802.11), All 11u Capable Clients, 802.11a/n, 802.11b/g/n, 802.11a, 802.11b, 802.11g, 802.11n (5 GHz), 802.11n (2.4 GHz).
- Reporting Period
 - Select the reporting period from the Select a time period...drop-down list. The possible values are Today, Last 1 Hour, Last 6 Hours, Last 12 hours, Last 1 Day, Last 2 Days, Last 3 days, Last 4 Days, Last 5 Days, last 6 Days, Last 7 Days, Last 2 Weeks, Last 4 weeks, Previous Calendar Month, Last 8 Weeks, Last 12 Weeks, Last 6 Months, and Last 1 Year.
 - From—Select the **From** radio button and enter the From and To dates and times. You can type a date in the text box, or click the **Calendar** icon to choose a date. Choose the hours and minutes from the drop-down lists.
- Show—Enter the number of records that you want to be displayed on each page.



Note Leave the text box blank to display all records.

Step 5 If you plan to run this report at a later time or as a recurring report, enter the Schedule parameters. The Schedule parameters allow you to control when and how often the report runs.

- Scheduling—Select the **Enable** check box to run the report on the set schedule.
- Export Format—Choose your format for exported files (**CSV** or **PDF**).
- Destination—Select your destination type (**File** or **E-mail**). Enter the applicable file location or the e-mail address.



Note The default file locations for CSV and PDF files are as follows:

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



Note To set the mail server setup for e-mails, choose **Administration > Settings**, then choose **Mail Server** from the left sidebar menu to view the Mail Server Configuration page. Enter the SMTP and other required information.

- Start Date/Time—Enter a date in the provided text box, or click the **calendar** icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists. The report begins to run on this data and at this time.
- Recurrence—Enter the frequency of this report.
 - No Recurrence—The report runs only once (at the time indicated for the Start Date/Time).
 - Hourly—The report runs on the interval indicated by the number of hours you enter in the Entry text box.
 - Daily—The report runs on the interval indicated by the number of days you enter in the Every text box.
 - Weekly—The report runs on the interval indicated by the number of weeks you enter in the Every text box and on the days specified by the selected check boxes.
 - Monthly—The report runs on the interval indicated by the number of months you enter in the Every text box.

The Create Custom Report page allows you to customize the report results. [Table 11-2](#) specifies which reports are customizable, which have multiple sub-reports, and which report views are available. In future releases, all reports are customizable.

Table 11-2 Report Customization

Report	Customizable?	Multiple Sub-Reports?	Report Views	Data Field Sorting?
Air Quality vs Time	Yes	No	Tabular	No
Security Risk Interferers	Yes	No	Tabular	No
Worst Air Quality APs	Yes	No	Tabular	No
Worst Interferers	Yes	No	Tabular	No
Busiest Clients	Yes	No	Tabular	No

Table 11-2 Report Customization (continued)

Report	Customizable?	Multiple Sub-Reports?	Report Views	Data Field Sorting?
Client Count	Yes	No	Graphical	No
Client Session	Yes	No	Tabular	No
Client Summary	Yes	Yes	Various	Yes
Client Traffic	Yes	No	Graphical	No
Client Traffic Stream Metrics	Yes	No	Tabular ¹	No
Throughput	No	No	Tabular	No
Unique Clients	Yes	No	Tabular	No
v5 Client Statistics	No	No	Tabular	No
Configuration Audit	Yes	No	Tabular	No
PCI DSS Detailed	Yes	No	Tabular	No
PCI DSS Summary	Yes	No	Graphical	No
AP Profile Status	Yes	No	Tabular	No
Device Summary	Yes	No	Tabular	No
Busiest APs	Yes	No	Tabular	No
Inventory - Combined Inventory	Yes	Yes	Various ²	Yes
Inventory - APs	Yes	Yes	Various	Yes
Inventory - Controllers	Yes	Yes	Various	Yes
Inventory - MSEs	Yes	Yes	Various	Yes
Up Time	Yes	No	Tabular	No
Utilization - Controllers	No	No	Graphical	No
Utilization - MSEs	No	No	Graphical	No
Utilization - Radios	No	No	Graphical	No
Guest Account Status	Yes	No	Tabular	No
Guest Association	Yes	No	Tabular	No
Guest Count	No	No	Tabular	No
Guest User Sessions	Yes	No	Tabular	No
Prime Infrastructure Guest Operations	Yes	No	Tabular	No
Alternate Parent	Yes	No	Tabular	No
Link Stats - Link Stats	Yes	No	Tabular	No
Link Stats - Node Hops	Yes	No	Graphical	No
Nodes	Yes	No	Tabular	No
Packet Stats - Packet Stats	No	No	Graphical	No

Table 11-2 Report Customization (continued)

Report	Customizable?	Multiple Sub-Reports?	Report Views	Data Field Sorting?
Packet Stats - Packet Error Stats	No	No	Graphical	No
Packet Stats - Packet Queue Stats	No	No	Graphical	No
Stranded APs	No	No	Tabular	No
Worst Node Hops - Worst Node Hop	Yes	Yes	Various	No
Worst Node Hops - Worst SNR Link	Yes	Yes	Various	No
802.11n Summary	No	Yes	Graphical	No
Executive Summary	No	Yes	Various	No
802.11 Counters	Yes	No	Both	Yes
Coverage Holes	Yes	No	Tabular	No
Network Utilization	Yes	Yes	Both	Yes
Traffic Stream Metrics	Yes	Yes	Both	Yes
Tx Power and Channel	No	No	Graphical	No
VoIP Calls Graph	No	No	Graphical	No
VoIP Calls Table	No	No	Tabular	No
Voice Statistics	No	No	Graphical	No
Adaptive wIPS Alarm	Yes	No	Tabular	No
Adaptive wIPS Alarm Summary	Yes	No	Both	No
Adaptive wIPS Top 10 APs	Yes	No	Tabular	No
Adhoc Rogue Count Summary	Yes	No	Both	No
Adhoc Rogues	Yes	No	Tabular	No
New Rogue AP Count Summary	Yes	No	Both	No
New Rogue APs	No	No	Graphical	No
Rogue AP Count Summary	Yes	No	Both	No
Rogue APs	Yes	No	Tabular	No
Security Alarm Trending Summary	Yes	No	Graphical	No

1. Sub-report Client Summary view is tabular only. The rest of the sub-reports such as Client Summary by Protocol have both report views and are customizable to show either tabular, graphical, or both.
2. Combined inventory (similar to other inventory reports: APs/Controllers/MSEs) consists of multiple sub-reports. Reports that are by model or version have both views. These views are customizable with setting such as Count of Controllers by Model. Other reports, such as Controller Inventory, are tabular only.

Step 6 Click **Customize** to open a separate Create Custom Report page (see [Figure 11-3](#)).

Figure 11-3 *Customize Report View Page*

- a. From the Custom Report Name drop-down list, choose the report you intend to run. The Available and Selected column heading selections may change depending on the report selected.
- b. From the Report View drop-down list, specify if the report should appear in tabular, graphical, or combined form (both). This option is not available on every report.
- c. Use the **Add >** and **< Remove** buttons to move highlighted column headings between the two group boxes (Available data fields and Data fields to include).



Note Column headings in **blue** are mandatory in the current sub report. They cannot be removed from the Selected Columns group box.

- d. Use the **Change Order** buttons (Move Up or Move Down) to determine the order of the columns in the results table. The higher the column heading appears in the Selected Columns list, the farther left it appears in the results table.
- e. In the Data field sorting group box, indicate your sorting preference (Ascending or Descending). Determine how the report data is sorted.
 - You can select four data fields for which you can specify sorting order. Use the Sort by and Then by drop-down lists to select each data field for sorting.
 - For each sorted data field, select whether you want it sorted in Ascending or Descending order.



Note Only reports in table form (rather than graphs or combined) can be sorted. Only fields that can be sorted appear in the Data field sorting drop-down lists.

- f. Click **Apply** to confirm the changes, **Reset** to return columns to the default, or **Cancel** to close this page with no changes made.



Note The changes made in the Create Custom Report page are not saved until you click **Save** in the Report Details page.

- Step 7** When all report parameters have been set, choose one of the following:
- **Save**—Click **Save** to save this report setup without immediately running the report. The report automatically runs at the scheduled time.
 - **Save and Run**—Click **Save and Run** to save this report setup and to immediately run the report.
 - **Run Now**—Click **Run Now** to run the report without saving the report setup.
 - **Cancel**—Click **Cancel** to return to the previous page without running nor saving this report.

Managing Current Reports

If a report has been saved for a specific report type, you can access the current reports from the Report Launch Pad.

To access current or saved reports from the Report Launch Pad, follow these steps:

- Step 1** Choose **Reports > Report Launch Pad**.
- Step 2** Choose the specific report from the left sidebar menu or from the main section of the Report Launch Pad. The Report Launch Pad page displays a list of current reports for this report type.



Note To view a list of saved reports, choose **Reports > Saved Reports**. See the [“Managing Saved Reports” section on page 11-16](#) for more information.

Managing Scheduled Run Results

To view all currently scheduled runs in the Prime Infrastructure, choose **Report > Scheduled Run Results**. This section contains the following topics:



Note The list of scheduled runs can be sorted by report category, report type, and time frame.

The Scheduled Run Results page shows the following information:

- **Report Title**—Identifies the user-assigned report name.



Note Click the report title to view the details for this report.

- **Report Type**—Identifies the specific report type.
- **Status**—Indicates whether or not the report ran successfully.

- **Message**—Indicates whether or not this report was saved and the filename for this report (if saved).
- **Run Date/Time**—Indicates the date and time that the report is scheduled to run.
- **History**—Click the **History** icon to view all scheduled runs and their details for this report.
- **Download**—Click the **Download** icon to open or save a .csv/.pdf file of the report results.

For more information about scheduled run results, see the [“Viewing or Editing Scheduled Run Details” section on page 11-16](#).

Sorting Scheduled Run Results

You can use the Show drop-down list to sort the Scheduled Run Results by category, type, and time frame:

- **Report Category**—Choose the appropriate report category from the drop-down list or choose **All**.
- **Report Type**—Choose the appropriate report type from the drop-down list or choose **All**. The report Type selections change depending on the selected report category.
- **From/To**—Type the report start (From) and end (To) dates in the text boxes, or click the **calendar** icons to select the start and end dates.
- **Report Generation method**—Choose the appropriate report generation method from the drop-down list. The possible methods are **Scheduled**, **On-demand Export**, and **On-demand Email**.

Click **Go** to sort this list. Only reports that match your criteria appear.

Viewing or Editing Scheduled Run Details

To view or edit a saved report, follow these steps:

-
- Step 1** Choose **Report > Scheduled Run Results**.
 - Step 2** Click the **Report Title** link for the appropriate report to open the Report Details page.
 - Step 3** In this page, you can view or edit the details for the scheduled run.
 - Step 4** When all scheduled run parameters have been edited (if necessary), select from the following:
 - **Save**—Click **Save** to save this schedule run without immediately running the report. The report automatically runs at the scheduled time.
 - **Save and Run**—Click **Save and Run** to save this scheduled run and to immediately run the report.
 - **Cancel**—Click **Cancel** to return to the previous page without running nor saving this report.
 - **Delete**—Click **Delete** to delete the current saved report.
-

Managing Saved Reports

In the Saved Reports page, you can create and manage saved reports. To open this page in the Prime Infrastructure, choose **Reports > Saved Reports**.



Note

The list of saved reports can be sorted by report category, report type, and scheduled status (enabled, disabled, or expired).

The Saved Reports page shows the following information:

- Report Title—Identifies the user-assigned report name.



Note Click the report title to view the details for this report.

- Report Type—Identifies the specific report type.
- Scheduled—Indicates whether this report is enabled or disabled.
- Next Schedule On—Indicates the date and time of the next scheduled run for this report.
- Last Run—Indicates the date and time of the most recent scheduled run for this report.
- Download—Click the **Download** icon to open or save a .csv file of the report results.
- Run Now—Click the **Run Now** icon to immediately run the current report.

For additional information on saved reports, see the “[Sorting Saved Reports](#)” section on page 11-17.

Sorting Saved Reports

You can use the Show drop-down lists to sort the saved Reports list by category, type, and scheduled status (see [Figure 11-4](#)).

- Report Category—Choose the appropriate report category from the drop-down list or choose **All**.
- Report Type—Choose the appropriate report type from the drop-down list or choose **All**. The Report Type selections change depending on the selected report category.
- Scheduled—Choose **All**, **Enabled**, **Disabled**, or **Expired** to sort the Saved Reports list by scheduled status.

Figure 11-4 *Sorting Saved Reports*

Saved Reports
[Report Launch Pad](#) > **Saved Reports**

Report Category	Report Type	Scheduled	Go
Show: Security	All	All	Go
<input type="checkbox"/> Report Title ^	Rep		Next S
<input type="checkbox"/> AQVSTime	Air C	d	
<input type="checkbox"/> All record report	Wor	d	
<input type="checkbox"/> worst AQ per floor	Wor	d	
<input type="checkbox"/> worst air report	Wor	d	Wed J 25:18:61

Click **Go** to sort this list. Only reports that match your criteria appear.

Viewing or Editing Saved Report Details

To view or edit a saved report, follow these steps:

- Step 1** Choose **Report > Saved Reports**.
- Step 2** Click the **Report Title** link for the appropriate report to open the Report Details page.
- Step 3** In the Report Details page, you can view or edit the details for the saved report.

- Step 4** When all report parameters have been edited, choose one of the following:
- **Save**—Click **Save** to save this report setup without immediately running the report. The report automatically runs at the scheduled time.
 - **Save and Run**—Click **Save and Run** to save this report setup and to immediately run the report.
 - **Run Now**—Click **Run Now** to run the report without saving the report setup.
 - **Cancel**—Click **Cancel** to return to the previous page without running nor saving this report.
 - **Delete**—Click **Delete** to delete the current saved report.

Generating MSE Analytics Reports

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

To generate a MSE analytics report, click **New** that is next to a type to create a new report. See “[Managing Saved Reports](#)” section on page 11-16 for more information.

Click a report type to view currently saved reports. In this page, you can enable, disable, delete, or run currently saved reports. See the “[Managing Current Reports](#)” section on page 11-15 for more information.

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

- [Client Location, page 11-18](#)
- [Client Location Density, page 11-20](#)
- [Device Count by Zone, page 11-21](#)
- [Device Dwell Time by Zone, page 11-23](#)
- [Guest Location Density, page 11-25](#)
- [Location Notifications by Zone, page 11-26](#)
- [Mobile MAC Statistics, page 11-28](#)
- [Rogue AP Location Density, page 11-29](#)
- [Rogue Client Location Density, page 11-31](#)
- [Tag Location, page 11-32](#)
- [Tag Location Density, page 11-34](#)

Client Location

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

**Note**

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

This section contains the following topics:

- [Configuring a Client Location Report, page 11-19](#)
- [Client Location Results, page 11-19](#)

Configuring a Client Location Report

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

Settings

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



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

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



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

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the [“Managing Saved Reports” section on page 11-16](#) for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the [“Managing Saved Reports” section on page 11-16](#) for more information on customizing report results.



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

Client Location Results

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

- Last Located—The time when the client was located.
- Client Location—The position of the client at the located time.
- MSE—The name of the MSE that located this client.
- User—The username of the client.
- Detecting Controllers—The IP address of the detecting controller.

- 802.11 State—The state of 802.11. It can be either Probing or Associated.
- IP Address—The IP address of the client.
- AP MAC Address—The MAC address of the associated access point.
- Authenticated—Whether authenticated or not. This can be either Yes or No.
- SSID—The SSID used by the client.
- Protocol—The protocol used to retrieve the information from the client.

**Note**

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

Client Location Density

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

This section contains the following topics:

- [Configuring a Client Location Density Report, page 11-20](#)
- [Client Location Density Results, page 11-21](#)

Configuring a Client Location Density Report

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

- [“Settings” section on page 11-20](#)
- [“Schedule” section on page 11-21](#)
- [“Customize Report Form” section on page 11-21](#)

Settings

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

**Note**

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

- Reporting Period
 - Select the radio button and choose a period of time from the drop-down list.

or

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



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

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the [“Managing Saved Reports” section on page 11-16](#) for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the [“Managing Saved Reports” section on page 11-16](#) for more information on customizing report results.



Note

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

Client Location Density Results

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

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



Note

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

Device Count by Zone

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

This sections contains the following topics:

- [Configuring a Device Count by Zone Report, page 11-22](#)
- [Device Count by Zone Results, page 11-23](#)

Configuring a Device Count by Zone Report

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

- [Settings, page 11-22](#)
- [Schedule, page 11-23](#)
- [Customize Report Form, page 11-23](#)

Settings

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



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

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



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

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the [“Managing Saved Reports” section on page 11-16](#) for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the [“Managing Saved Reports” section on page 11-16](#) for more information on customizing report results.

**Note**

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

Device Count by Zone Results

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

- MSE—The name of the MSE that located this client
- Zone—Device count by zone results
- Device Type—Type of the device
- MSE Analytics Report Link—Link to get the MSE analytics report

Device Dwell Time by Zone

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

This sections contains the following topics:

- [Configuring a Device Count by Zone Report, page 11-22](#)
- Device Count by Zone Results

Configuring a Device Dwell Time by Zone Report

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

- [Settings, page 11-22](#)
- [Schedule, page 11-23](#)
- [Customize Report Form, page 11-23](#)

Settings

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



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

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



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

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the [“Managing Saved Reports” section on page 11-16](#) for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the [“Managing Saved Reports” section on page 11-16](#) for more information on customizing report results.



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

Device Dwell Time by Zone Results

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

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

Guest Location Density

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

This section contains the following topics:

- [Configuring Guest Location Tracking, page 11-25](#)
- [Guest Location Tracking Results, page 11-26](#)

Configuring Guest Location Tracking

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

- “Settings” section on page 11-25
- “Schedule” section on page 11-25
- “Customize Report Form” section on page 11-26

Settings

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



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

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



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

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the “[Managing Saved Reports](#)” section on page 11-16 for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the [“Managing Saved Reports” section on page 11-16](#) for more information on customizing report results.

**Note**

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

Guest Location Tracking Results

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

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

**Note**

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

Location Notifications by Zone

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

**Note**

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

This section contains the following topics:

- [Configuring a Location Notification Report, page 11-26](#)
- [Location Notification Results, page 11-28](#)

Configuring a Location Notification Report

- This section describes how to configure a Location Notification report and contains the following topics:

- [Schedule, page 11-27](#)
- [Customize Report Form, page 11-28](#)

Settings

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



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

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



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

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the [“Managing Saved Reports” section on page 11-16](#) for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the [“Managing Saved Reports” section on page 11-16](#) for more information on customizing report results.



Note

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

Location Notification Results

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

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

Mobile MAC Statistics

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

- [Configuring Rogue AP Location Tracking, page 11-30](#)
- [Rogue AP Location Tracking Results, page 11-31](#)

Configuring Mobile MAC Statistics

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

- [“Settings” section on page 11-30](#)
- [“Schedule” section on page 11-30](#)
- [“Customize Report Form” section on page 11-30](#)

Settings

- Report Title—If you plan to save this report, enter a report name.
- Report by
 - MSE By Floor Area
 - MSE By Outdoor Area
 - MSE

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



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

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



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

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the [“Managing Saved Reports” section on page 11-16](#) for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the [“Managing Saved Reports” section on page 11-16](#) for more information on customizing report results.



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

Mobile MAC Statistics

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

- Venue
- Click Count
- Mobile MAC Address



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

Rogue AP Location Density

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

This section contains the following topics:

- [Configuring Rogue AP Location Tracking, page 11-30](#)

- [Rogue AP Location Tracking Results, page 11-31](#)

Configuring Rogue AP Location Tracking

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

- [“Settings” section on page 11-30](#)
- [“Schedule” section on page 11-30](#)
- [“Customize Report Form” section on page 11-30](#)

Settings

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



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

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



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

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the [“Managing Saved Reports” section on page 11-16](#) for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the [“Managing Saved Reports” section on page 11-16](#) for more information on customizing report results.



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

Rogue AP Location Tracking Results

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

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

**Note**

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

Rogue Client Location Density

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

This section contains the following topics:

- [Configuring a Rogue Client Location Tracking, page 11-31](#)
- [Rogue Client Location Tracking Results, page 11-32](#)

Configuring a Rogue Client Location Tracking

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

- “Settings” section on page 11-31
- “Schedule” section on page 11-32
- “Customize Report Form” section on page 11-32

Settings

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

**Note**

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

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



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

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the [“Managing Saved Reports” section on page 11-16](#) for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the [“Managing Saved Reports” section on page 11-16](#) for more information on customizing report results.



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

Rogue Client Location Tracking Results

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

- Last Located—The time when the rogue client was last located during the selected Report Time criteria.
- MAC Address—The MAC address of the rogue client.
- Rogue Client Location—The position of the rogue client at the located time.
- MSE—The name of the MSE that located this rogue client.
- Rogue AP—The rogue access point to which the rogue client is associated with.
- Detecting Controllers—The IP address of the detecting controller.
- State—The state of the Rogue client.



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

Tag Location

This report shows the location history of a tag detected by an MSE.

This section contains the following topics:

- [Configuring a Tag Location Tracking, page 11-34](#)

- [Tag Location Tracking Results, page 11-35](#)

Configuring Tag Location History

This section describes procedures to configure a Tag Location History report and contains the following topics:

- [“Settings” section on page 11-33](#)
- [“Schedule” section on page 11-33](#)
- [“Customize Report Form” section on page 11-33](#)

Settings

- Report Title—If you plan save this report, enter a report name.
- Report by
 - Tag MAC address.
- Report Criteria—Click **Edit** and enter a valid Tag MAC address as the filter criteria.



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

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



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

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the [“Managing Saved Reports” section on page 11-16](#) for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the [“Managing Saved Reports” section on page 11-16](#) for more information on customizing report results.



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

Tag Location History Results

The results of Tag Location History report contains the following information:

- Last Located—The time when the tag was last located during the selected Report Time criteria.
- Tag Location—The position of the tag at the located time.
- MSE—The name of the MSE that located this tag.
- Detecting Controller—The IP address of the detecting controller.
- Vendor—The name of the vendor for the client.
- Battery Status—The battery status of the client.

**Note**

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

Tag Location Density

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

This section contains the following topics:

- [Configuring a Tag Location Tracking, page 11-34](#)
- [Tag Location Tracking Results, page 11-35](#)

Configuring a Tag Location Tracking

This section describes procedures to configure a Tag Location Tracking report and contains the following topics:

Settings

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

**Note**

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

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



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

Schedule

If you plan to run this report at a later time or as a recurring report, enter the scheduling parameters. See the [“Managing Saved Reports” section on page 11-16](#) for more information on scheduling a report.

Customize Report Form

The Customize Report form allows you to customize the report results. See the [“Managing Saved Reports” section on page 11-16](#) for more information on customizing report results.



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

Tag Location Tracking Results

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

- Last Located—The time when the tag was last located during the selected Report Time criteria.
- Tag Location—The position of the tag at the located time.
- MSE—The name of the MSE that located this tag.
- Detecting Controller—The IP address of the detecting controller.
- Vendor—The name of the tag vendor.
- Battery Status—The status of the battery of that tag.



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

Creating a Device Utilization Report

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

- Step 1** Choose **Reports > Report Launch Pad**.
- Step 2** Choose **Device > Utilization**.
- Step 3** Click **New**. The Utilization Report Details page appears.
- Step 4** In the Reports Details page, enter the following Settings parameters:



Note Certain parameters may or may not work depending on the report type.

- Report Title—If you plan to save this report, enter a report name.
- Report Type—By default, the report type is selected as MSE.

- Report By—Choose the appropriate Report By category from the drop-down list. The categories differ for each report. See specific report sections for Report By categories for each report.
- Report Criteria—The parameter allows you to sort your results depending on the previous Report By selection made. Click **Edit** to open the Filter Criteria page.
- Connection Protocol—Choose one of these protocols: **All Clients**, **All Wired (802.3)**, **All Wireless (802.11)**, **802.11a/n**, **802.11b/g/n**, **802.11a**, **802.11b**, **802.11g**, **802.11n (5-GHz)**, or **802.11n (2.4-GHz)**.
- SSID—All SSIDs is the default value.
- Reporting Period—You can define the report to collect data hourly, weekly, or at a specific date and time. The selected reporting period type is displayed on the x-axis.



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

Step 5 In the Schedule group box, select the **Enable Schedule** check box.

Step 6 Choose the report format (**CSV** or **PDF**) from the Export Report drop-down list.

Step 7 Select either **File** or **Email** as the destination of the report.

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

Step 8 Enter a start date (MM:DD:YYYY), or click the **calendar** icon to select a date.

Step 9 Specify a start time using the hour and minute drop-down list boxes.

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

- No Recurrence
- Hourly
- Daily
- Weekly
- Monthly



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

Step 11 When finished with [Step 1](#) to [Step 10](#), do one of the following:

- Click **Save** to save edits. The report is run at the designated time and the results are either e-mailed or saved to a designated file as defined in the Schedule group box.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any pending, scheduled run of that report. Results appear at the bottom of the page. The report also runs at the designated time and the results are either e-mailed or saved to a designated file as defined in the Schedule group box.
 - In the results page, click **Cancel** to cancel the defined report.

- Click **Run Now** if you want to run the report immediately and review the results in the Prime Infrastructure page. The report runs regardless of any pending, scheduled run of that report. Results appear at the bottom of the page. Click **Save** if you want to save the report criteria you entered.



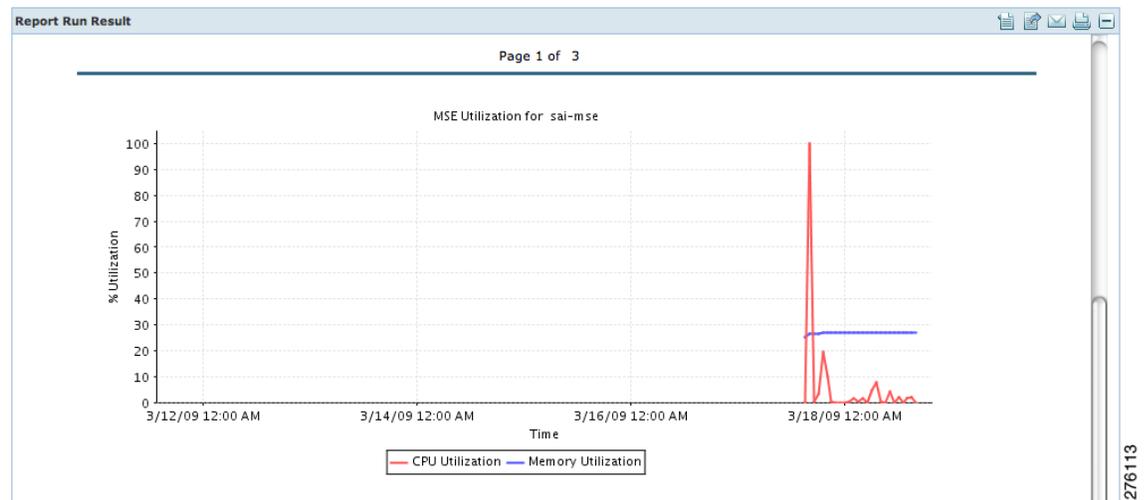
Note You can also click **Run Now** to check the defined report criteria before saving it or to run reports as necessary.

The results appear at the bottom of the page (see [Figure 11-5](#)).



Note Only the CPU and memory utilization reports are shown in the following example (see [Figure 11-5](#)).

Figure 11-5 Devise > MSE Utilization > Results



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

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

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

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

Step 13 To enable, disable, or delete a report, select the check box next to the report title and click the appropriate option.

Viewing Saved Utilization Reports

To download a saved report, follow these steps:

Step 1 Choose **Reports > Saved Reports**.

- Step 2** Click the **Download** icon for your report. It is downloaded and saved in the defined directory or e-mailed.
-

Viewing Scheduled Utilization Runs

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

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

Managing OUI

The Prime Infrastructure relies on the IEEE Organizational Unique Identifier (OUI) database to identify the client vendor name mapping. Prime Infrastructure stores vendor OUI mappings in an XML file named vendorMacs.xml. This file is updated for each release of Prime Infrastructure. With the OUI update, you can perform the following:

- Change the vendor display name for an existing OUI.
- Add new OUIs to Prime Infrastructure.
- Refresh the vendorMacs.xml file with new vendor OUI mappings and upload it to Prime Infrastructure.

This section contains the following topics:

Adding a New Vendor OUI Mapping

The User Defined OUI List page displays a list of vendor OUI mappings that you created. This page allows you to add a new vendor OUI mapping, delete an OUI entry, and update the vendor name for an OUI that is existing in the vendorMacs.xml file.

When you add an OUI, Prime Infrastructure verifies the vendorMacs.xml file to see if the OUI exists. If the OUI exists, Prime Infrastructure updates the vendor name for the OUI. If the OUI does not exist, Prime Infrastructure adds a new OUI entry to the vendor OUI mapping.

To add a new vendor OUI mapping, follow these steps:

- Step 1** Choose **Administration > System Settings**.
- Step 2** From the left sidebar menu, choose **User Defined OUI**. The User Defined OUI page appears.
- Step 3** From the Select a Command drop-down list, choose **Add OUI Entries**, and Click **Go**.
- Step 4** In the OUI field, enter a valid OUI. The format is aa:bb:cc.
- Step 5** Click **Check** to verify if the OUI exists in the vendor OUI mapping.
- Step 6** In the Name field, enter the display name of the vendor for the OUI.

- Step 7** Select the **Change Vendor Name** check box to update the display name of the vendor, if the OUI exists in the vendor OUI mapping.
- Step 8** Click **OK**.
-

Uploading an Updated Vendor OUI Mapping File

The updated vendorMacs.xml file is posted on cisco.com, periodically. You can download and save the file to a local directory using the same filename, vendorMacs.xml. You can then, upload the file to Prime Infrastructure. Prime Infrastructure replaces the existing vendorMacs.xml file with the updated file and refreshes the vendor OUI mapping. However, it does not override the new vendor OUI mapping or the vendor name update that you made.

To upload the updated vendor OUI mapping file, follow these steps:

- Step 1** Choose **Administration > System Settings**.
- Step 2** From the left sidebar menu, choose **Upload OUI**. The Upload OUI From File page appears.
- Step 3** Browse and select the vendorMacs.xml file that you downloaded from Cisco.com.
- Step 4** Click **OK**.
-

Monitoring Wireless Clients

This section describes about monitoring wireless clients and contains the following topics:

- [Monitoring Wireless Clients Using Maps, page 11-39](#)
- [Monitoring Wireless Clients Using Search, page 11-40](#)

Monitoring Wireless Clients Using Maps

On the Prime Infrastructure map, you can view the name of the access point that the client is associated with, the IP Address, Asset information, Authentication, SSID, 802.11 protocol, and when the location information was last updated for the client. Hover your mouse cursor over the client icon on the map to display this information.

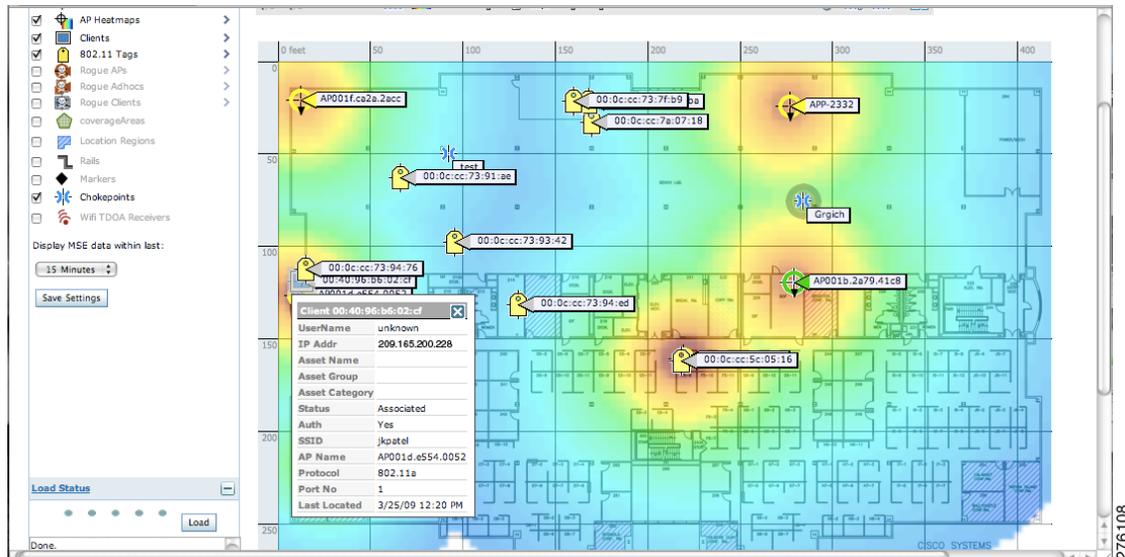
You can also view the client details page, that provides statistics (such as client association, client RSSI, and client SNR), packets transmitted and received values, events, and security information for that client.

To determine the location status of a client on a map and view its client details page using maps, follow these steps:

- Step 1** Choose **Monitor > Site Maps**.
- Step 2** Choose the building and floor on which the mobility services engine and its clients are located.
- Step 3** Select the **Clients** check box in the Floor Settings left sidebar menu, if it is not already selected (see [Figure 11-6](#)).

Do not click **Save Settings** unless you want to save changes made to the floor settings across all maps.

Figure 11-6 Monitor > Maps > Building > Floor Page



Note The map shows only associated clients by default. To see clients in all state, choose the **show all clients** option.



Note The map shows clients that was visible in the last 15 minutes. This value can be changed using the drop-down list in the left sidebar menu of the Maps page.

Step 4 Hover your mouse cursor over a client icon (blue square) and a summary of its configuration appears in a pop-up dialog box.



Note You can enter a custom note for a client in the summary dialog box. You can also edit it in the Client Details page.

Step 5 Click the **Client** icon to see client details.

Step 6 Click the **More** link to configure asset information for the client.

Monitoring Wireless Clients Using Search

You can view client information in summary and in detail in the Monitor > Clients page and in the maps page (Monitor > Maps).

To view client information, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

The Clients and Users appears.

Step 2 From the Show drop-down list, choose **Clients Detected by MSEs**. Click **Go**.

A summary of all clients detected by mobility services engines and location appliances managed by Prime Infrastructure is displayed (see [Figure 11-6](#)). The clients detected by MSE is a union of wired and wireless clients.

Location information is stored only for wireless clients in MSE but not for wired clients. Hence, in order to filter clients by virtual domain, switch ports must be assigned to floors in the given virtual domain in order to view the wired clients, otherwise only wireless clients are listed here.



Note The clients will only show one IP address when you hover your mouse over the client to see the information, even though there might be multiple IP addresses associated with this client. The details page will show all the IP addresses. Also the clients displayed can be filtered using any of the multiple IP addresses that a client can have (full or partial). the IP address displayed is the best matched string searched.

- a. To find a specific client by its IP address, name, SSID, or MAC address, enter that value into the Search text box in the navigation bar (not all search values apply to all clients).
For example, if you enter a MAC address in the Search text box, the following page appears.
- b. To see more configuration details about the client, click **View List** for the client item type. Details shown include associated devices (access point, controller), map location, VLAN, protocol, and authentication type.
- c. To see alarms for the client, click **View List** for the alarm item type. A listing of all active alarms for that client noting severity, failure source (alarm description), owner of alarm (if assigned), date and time of the alarm, and whether or not alarm is acknowledged.



Note You can also assign or unassign the alarm, e-mail it, delete or clear it, and acknowledge and unacknowledge it in this page by choosing the appropriate option from the Select a command drop-down list.

- d. To search for a client or multiple clients by device, network, map location and type of client (regular, rogue, or shunned), click the **Advanced Search** link.

You can further define the client category by all clients, all excluded clients, all wired guest clients, and all logged in clients using the Search By drop-down list.

Click the appropriate client.

Client Support on the MSE

You can use the Prime Infrastructure Advanced Search feature to narrow the client list based on specific categories and filters.

This section contains the following topics:

- [Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address](#), page 11-42

- [Viewing the Clients Detected by the MSE, page 11-43](#)

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



Note Only wireless clients have IPv6 addresses in this release.

To search for an MSE-located client using the Prime Infrastructure Advanced Search feature, follow these steps:

Step 1 Click **Advanced Search** located in the top right corner of the Prime Infrastructure UI.

Step 2 Choose **Clients** as the search category from the Search Category drop-down list.

Step 3 From the Media Type drop-down list, choose **Wireless Clients**.



Note The Wireless Type drop-down list appears only when you choose Wireless Clients as the media type.

Step 4 From the Wireless Type drop-down list, choose any of the following types: **All**, **Lightweight**, or **Autonomous Clients**.

Step 5 From the Search By drop-down list, choose **IP Address**.



Note Searching a client by IP address can contain either a full or partial IP address. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

Step 6 From the Clients Detected By drop-down list, choose **clients detected by MSE**.

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

Step 7 From the Last detected within drop-down list, choose the time within which the client was detected.

Step 8 Enter the client IP address in the Client IP Address text box. You can enter wither a partial or full IPv6 address.



Note If you are searching for the client from the Prime Infrastructure on the MSE by IPV4 address, enter the IPV4 address in the Client IP address text box.

Step 9 From the Client States drop-down list, choose the client states. The possible values for wireless clients are **All States**, **Idle**, **Authenticated**, **Associated**, **Probing**, or **Excused**. The possible values for wired clients are **All States**, **Authenticated**, and **Associated**.

Step 10 From the Posture Status drop-down list, choose the posture status to know if the devices are clean or not. The possible values are **All**, **unknown**, **Passed**, and **Failed**.

- Step 11** Select the **CCX Compatible** check box to search for clients that are compatible with Cisco Client Extensions. The possible values are **All Versions**, **V1**, **V2**, **V3**, **V4**, **V5**, and **V6**.
- Step 12** Select the **E2E Compatible** check box to search for clients that are End to End compatible. The possible values are **All Versions**, **V1**, and **V2**.
- Step 13** Select the **NAC State** check box to search for clients identified by a certain Network Admission Control (NAC) state. The possible values are **Quarantine**, **Access**, **Invalid**, and **Not Applicable**.
- Step 14** Select the **Include Disassociated** check box to include clients that are no longer on the network but for which the Prime Infrastructure has historical records.
- Step 15** From the **Items per page** drop-down list, choose the number of records to be displayed in the search results page.
- Step 16** Select the **Save Search** check box to save the selected search option.
- Step 17** Click **Go**.
- The Clients and Users page appears with all the clients detected by the MSE.
-

Viewing the Clients Detected by the MSE

To view all the clients detected by the MSE, follow these steps:

- Step 1** Choose **Monitor > Clients and Users** to view both wired and wireless clients information.
- The Client and Users page appears.
- The Clients and Users table shows a few column by default. If you want to display the additional columns that are available, click  , and then click **Columns**. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.
- Step 2** Filter the current list to choose all the clients that are detected by the MSE by choosing **Clients detected by MSE** from the Show drop-down list.

All the clients detected by the MSE including wired and wireless appear.

The following different parameters are available in the Clients Detected by MSE table:

- MAC Address—Client MAC address.
- IP Address—Client IP address.

The IP address that appears in the IP Address column is determined by a predefined priority order. The first IP address available in the following order appears in the IP address text box:

- IPv4 address



Note Only wireless clients have IPv6 addresses in this release. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

- IPv6 global unique address. If there are multiple addresses of this type, the most recent IPv6 address that the client received is shown, because a user might have two Global IPv6 addresses but one might have been from an older Router Advertisement that is being aged out.

- IPv6 local unique address. If there are multiple addresses, then the most recent IPV6 local unique address is used by the client.
- IPv6 link local address. For an IPv6 address of the client, which is self-assigned and used for communication before any other IPV6 address is assigned.

The following are the different IPv6 address types:

- Link-local Unicast—The link-local addresses are designed to be used for addressing on a single link for purposes such as auto-address configuration, neighbor discovery, or when no routers are present.
- Site-local Unicast—The site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix.
- Aggregatable Global Unicast—The aggregatable global unicast address uniquely identifies the client in global network and equivalent to public IPv4 address. A client can have multiple aggregatable global unicast addresses.
- IP Type—The IP address type of the client. The possible options are IPv4, IPv6, or Dual-stack that signifies a client with both a IPV4 and IPV6 addresses.
 - Global Unique
 - Unique Local
 - Link Local
- User Name—Username based on 802.1x authentication. Unknown is displayed for client connected without a username.
- Type—Indicates the client type.
 -  Indicates a lightweight client
 -  Indicates a wired client
 -  Indicates an autonomous client
- Vendor—Device vendor derived from OUI.
- Device Name—Network authentication device name. For example, WLC and switch.
- Location—Map location of the connected device.
- VLAN—Indicates the access VLAN ID for this client.
- Status—Current client status.
 - Idle—Normal operation; no rejection of client association requests.
 - Auth Pending—Completing a AAA transaction.
 - Authenticated—802.11 authenticated complete.
 - Associated—802.11 association complete. This is also used by wired clients to represent that a client is currently connected to the network.
 - Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.
 - To Be Deleted—The client is deleted after disassociation.
 - Excluded—Automatically disabled by the system due to perceived security threat.
- Interface—Controller interface (wireless) or switch interface (wired) that the client is connected to.
- Protocol
 - 802.11—Wireless

- 802.3—Wired
- Association Time—Last association start time (for wireless client). For a wired client, this is the time when a client is connected to a switch port. This is blank for a client which is associated but has problems being on the network.
- CCX—Lightweight wireless only.

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

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



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

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

Client Attributes

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

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



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

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

- Windows AD Domain



Note The identity clients are clients whose authentication type is 802.1x, MAC Auth Bypass or Web Auth. For non-identity clients, the authentication type is N/A.



Note The data that appears under the client attributes differs based on identity and non-identity clients. For identity clients, you can see the security information such as Authentication status, Audit Session ID, and so on.

- Statistics (wireless only)
- Traffic—Shows the client traffic information.
- For wireless clients, client traffic information comes from the controller. For wired clients, the client traffic information comes from the ISE, and you must enable accounting information and other necessary functions on the switches.

Statistics

The **Statistics** group box contains the following information for the selected client:

- Client AP Association History.
- Client RSSI History (dBm)—History of RSSI (Received Signal Strength Indicator) as detected by the access point with which the client is associated.
- Client SNR History—History of SNR (signal-to-noise ratio of the client RF session) as detected by the access point with which the client is associated.
- Bytes Sent and Received (Kbps)—Bytes sent and received with the associated access point.
- Packets Sent and Received (per sec)—Packets sent and received with the associated access point.
- Client Data rate

This information is presented in interactive graphs.

Client IPv6 Addresses

The Client IPv6 Address group box contains the following information for the selected client:

- IP Address—Shows the client IPv6 address.
- Scope—Contains 3 scope types: Global Unique, Local Unique, and Link Local.
- Address Type—Shows the address type.
- Discovery Time—Time when the IP was discovered.

Association History

The association history dashlet shows information regarding the last ten association times for the selected client. This information helps in troubleshooting the client.

The Association History dashlet contains the following information:

- Association Time
- Duration
- User Name
- IP Address

- IP Address Type
- AP Name
- Controller Name
- SSID

Events

The Events group box in the Client Details page displays all events for this client including the event type as well as the date and time of the event:

- Event Type
- Event Time
- Description

Map

Click **View Location History** to view the location history details of wired and wireless clients.

The following location history information is displayed for a wired or wireless client:

- Timestamp
 - State
 - Port Type
 - Slot
 - Module
 - Port
 - User Name
 - IP Address
 - Switch IP
 - Server Name
 - Map Location Civic Location
-

Configuring Buildings

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

This section contains the following topics:

- [Adding a Building to a Campus Map, page 11-49](#)
- [Viewing a Building, page 11-51](#)
- [Editing a Building, page 11-52](#)
- [Deleting a Building, page 11-52](#)
- [Moving a Building, page 11-53](#)

Adding a Building to a Campus Map

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

-
- Step 1** Choose **Monitor > Site Maps** to display the Maps page.
- Step 2** Click the desired campus. The **Site Maps > Campus Name** page appears.
- Step 3** From the Select a command drop-down list, choose **New Building** and click **Go**.
- Step 4** In the Campus Name > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:
- Enter the building name.
 - Enter the building contact name.
 - Enter the number of floors and basements.
 - Enter the horizontal position (distance from the corner of the building rectangle to the left edge of the campus map) and the vertical position (distance from the corner of the building rectangle to the top edge of the campus map) in feet.



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

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



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



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

- Click **Place** to put the building on the campus map. The Prime Infrastructure creates a building rectangle scaled to the size of the campus map.
- Click the building rectangle and drag it to the desired position on the campus map.



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

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



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

- Step 5** (Optional) To assign location presence information for the new outdoor area, do the following:
- a. Choose **Edit Location Presence Info** from the Select a command drop-down list. Click **Go**. The Location Presence page appears.
-  **Note** By default, the Presence Info check box of the Override Child Element is selected. This option should remain selected if you want to propagate the campus location to all buildings and floors on that campus. When adding buildings to the campus map, you can import the campus location information. The campus address cannot be imported to a building if the check box is unselected. This option should be unselected if you want to assign building-specific addresses to buildings on its campus rather than one campus address to all.
- b. Click the **Civic Address**, or **Advanced** tab.
 - Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
 - Advanced identifies the campus with expanded civic information such as neighborhood, city division, country, and postal community name.
 - c. By default, the Override Child's Presence Information check box is selected. There is no need to alter this setting for standalone buildings.
- Step 6** Click **Save**.

Adding a Standalone Building

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

- Step 1** Choose **Monitor > Site Maps** to display the Maps page.
- Step 2** From the Select a command drop-down list, choose **New Building**, and click **Go**.
- Step 3** In the Maps > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:
- a. Enter the building name.
 - b. Enter the building contact name.
-  **Note** After adding a new building, you can move it from one campus to another without having to recreate it.
- c. Enter the number of floors and basements.
 - d. Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.
-  **Note** To change the unit of measurement (feet or meters), choose **Monitor > Site Maps**, and choose **Properties** from the Select a command drop-down list.



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

- e. Click **OK** to save this building to the database.

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

- a. Choose **Location Presence** from the Select a command drop-down list. Click **Go**. The Location Presence page appears.
- b. Click the **Civic**, **GPS Markers**, or **Advanced** tab.
 - Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
 - GPS Markers identify the campus by longitude and latitude.
 - Advanced identifies the campus with expanded civic information such as neighborhood, city division, county, and postal community name.



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



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

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

Step 5 Click **Save**.



Note The standalone buildings are automatically placed in System Campus.

Viewing a Building

To view a current building map, follow these steps:

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

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



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

The map details include the following:

- Floor area
- Floor index—Indicates the floor level. A negative number indicates a basement floor level.
- Contact
- Status—Indicates the most serious level of alarm on an access point located on this map or one of its children.
- Number of total access points located on the map.
- Number of 802.11a/n and 802.11b/g/n radios located on the map.
- Number of out of service (OOS) radios.
- Number of clients—Click the number link to view the Monitor > Clients page.

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

- New Floor Area—See the [“Adding a Building to a Campus Map”](#) section on page 11-49 for more information.
 - Edit Building—See the [“Editing a Building”](#) section on page 11-52 for more information.
 - Delete Building—See the [“Deleting a Building”](#) section on page 11-52 for more information.
-

Editing a Building

To edit a current building map, follow these steps:

-
- Step 1** Choose **Monitor > Site Maps**.
 - Step 2** Click the name of the building map to open its details page.
 - Step 3** From the Select a command drop-down list, choose **Edit Building**.
 - Step 4** Make any necessary changes to Building Name, Contact, Number of Floors, Number of Basements, and Dimensions (feet).



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

Step 5 Click **OK**.

Deleting a Building

To delete a current building map, follow these steps:

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

- Step 2** Select the check box for the building that you want to delete.
- Step 3** Click **Delete** at the bottom of the map list (or choose **Delete Maps** from the Select a command drop-down list, and click **Go**).
- Step 4** Click **OK** to confirm the deletion.



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

Moving a Building

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

-
- Step 1** Choose **Monitor > Site Maps**.
- Step 2** Select the check box of the applicable building.
- Step 3** From the Select a command drop-down list, choose **Move Buildings**.
- Step 4** Click **Go**.
- Step 5** Choose the Target Campus from the drop-down list.
- Step 6** Select the buildings that you want to move. Unselect any buildings that remain in their current location.
- Step 7** Click **OK**.
-

Monitoring Tags

You can monitor tag status and location on the Prime Infrastructure maps as well as review tag details in the Monitor > Tags page. You can also use the Advanced Search to monitor tags.

This section contains the following topics:

- [Monitoring Tags Using Maps, page 11-53](#)
- [Monitoring Tags Using Search, page 11-54](#)
- [Overlapping Tags, page 11-57](#)

Monitoring Tags Using Maps

On the Prime Infrastructure map, you can view the name of the access point that generated the signal for a tagged asset, its strength of signal, and when the location information was last updated for the asset. Hover your mouse cursor over the tag icon on the map to display this information.

To enable tag location status on a map, follow these steps:

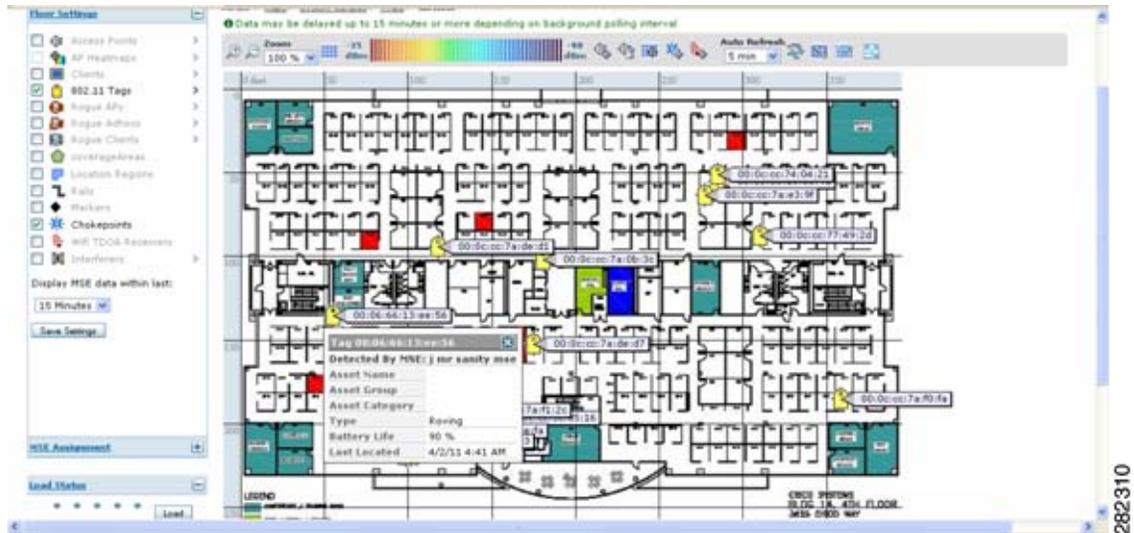
-
- Step 1** Choose **Monitor > Site Maps**.
- Step 2** Choose the building and floor on which the mobility services engine and tag are located.

- Step 3** Select the **802.11 Tags** check box in the Floor Settings menu if it is not already selected (see [Figure 11-7](#)).



Note Do not click **Save Settings** unless you want to save changes made to the floor settings across all maps.

Figure 11-7 Monitor > Maps > Building > Floor > Tag Page



- Step 4** Hover your mouse cursor over a tag icon (yellow tag) and a summary of its configuration appears in a Tag dialog box.
- Step 5** Click the **tag** icon to see tag details.
- You can also configure the asset information by entering the required information in the Asset Info group box.
- Step 6** To see location history for the tag, choose **Location History** from the Select a command drop-down list. Click **Go**.

Monitoring Tags Using Search

You can search for tags by asset type (name, category and group), MAC address, system (controller or MSE), and area (floor area and outdoor area).

You can further refine your search using the Advanced Search parameters and save the search criteria for future use. Click **Saved Searches** to retrieve saved searches.

When you click the MAC address of a tag location in a search results page, the following details appear for the tag:

- Tag vendor
- Controller to which tag is associated
- Telemetry data (CCX v1-compliant tags only)

- Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.
- Asset Information (Name, Category, Group)
- Statistics (Bytes and packets received)
- Location (Floor, Last Located, MSE, map)
- Location Notification (Absence, Containment, Distance, All)
- Emergency Data (CCX v1-compliant tags only)

To search for RFID tags, follow these steps:

Step 1 Choose **Monitor > RFID Tags**. The Tag Summary page appears.



Note Tags detected by MSE (in the last 15 minutes) display the total tag count equal to the number of tags by floors in the given virtual domain.

Step 2 To view a summary of tags associated with a specific mobility services engine, click the **Total Tags** link. The RFID Tags Summary page displays a list of tags by floors in the given domain.



Note If the listing of mobility services engines or tags is lengthy, you can use Search or Advanced Search to isolate a specific tag.



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

Step 3 To search for a specific tag, if you know its MAC address and asset name (not all search values apply to all tags), click the **Search** link.

Step 4 To search for a specific tag or multiple tags using a broader range of search criteria such as device (MSE or controller), map location (floor or outdoor area), asset name or category, or tag vendor, click the **Advanced Search** link.

- a. In the Advanced Search pane, select **Tags** as the search category.
- b. Select the additional tag search criteria. See [Table 11-3](#) for a list of search criteria and their possible values.

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

- c. Click **Go** when all advanced search parameters are selected.



Note If no tags are found based on the selected search criteria, a message appears noting this as well as the reason why the search was unsuccessful and possible actions.

Table 11-3 Tag Search Criteria and Values

Search Criteria	Variable Search Criteria	Possible Values
Search for tags by (Tier 1 search criteria)	—	All Tags; Asset Name, Asset Category or Asset Group; MAC Address; Controller or MSEs; Floor Area, or Outdoor Area. Note The MSE search includes both location servers and mobility services engines.
Search in (Tier 2 search criteria)	—	MSEs or Prime Infrastructure controllers. Note The Prime Infrastructure controller option indicates that the search for controllers is done within the Prime Infrastructure. Note The MSE search includes both location servers and mobility services engines.
Last detected within	—	Options are from 5 minutes to 24 hours.
Variable search criteria. (Tier 3 search criteria) Note Possible search criteria determined by the Search for tags by (Tier 1 search) value.	—	If the Search for tags by value is the following: <ol style="list-style-type: none"> 1. Asset Name, then enter tag asset name. 2. Asset Category, then enter tag asset category. 3. Asset Group, then enter tag asset group. 4. MAC Address, then enter tag MAC address. 5. Controller, then select controller IP address. 6. MSEs, then choose an MSE IP address from drop-down list. 7. Floor Area, then choose campus, building, and floor area. 8. Outdoor Area, then choose campus and outdoor area.
Telemetry tags only	—	Check box to display telemetry tags. Leaving option unselected shows all tags. Note Option only visible when the Search In option is MSE. Note Only those vendor tags that support telemetry appear.
Tag vendor	—	Check box to select tag vendor from drop-down list. Note Option only visible when the Search In option is MSE.
Items per page	—	Select the number of tags to display per search request. Values range from 10 to 500.
Save search	—	Check box to name and save search criteria. Once saved, entry appears under Saved Searches heading.

Overlapping Tags

When multiple tags are within close proximity of one another, a summary tag is used to represent their location on the Prime Infrastructure map (Monitor > Maps). The summary tag is labeled with the number of tags at that location.

When you hover your mouse cursor over the overlapping tag on the map, a dashlet appears with summary information for the overlapping tags.

Select the **Prev** and **Next** links to move between the individual tag summary dashlets. To see detailed information on a specific tag, select the **Details** link while viewing the summary information of the tag.

**Note**

- Summary information for tags includes Tag MAC address, Asset Name, Asset Group, Asset Category, Vendor (Type), Battery Life, and Last Located data (date and time). If the tag is Cisco CX v.1 compliant, telemetry information also appears.
- Detailed information for tags also includes the IP address of the associated controller, statistics, location notifications, location history, and whether the location debug feature is enabled.
 - To view location history for a tag, choose that option from the Select a command drop-down list, and click **Go**.
 - To return to the details page, choose Location History page from the Select a command drop-down list, and click **Go**.

Monitoring Chokepoints

A chokepoint must be assigned to a map for its location to be monitored. After adding the TDOA receiver to a map, you must resynchronize the network designs (Services > Synchronize Services) with the mobility services engine for it to appear on the map.

When a new chokepoint is created, it is available in all the virtual domains. After placing it on a floor, it is updated so that it is available in the same virtual domain as that of a floor. When a chokepoint is removed from a floor, it will be available in all the virtual domains again.

If the existing chokepoints are on a floor, then they all belong to the same virtual domain as the floor. If the chokepoints are not placed on a floor, then they are available in all virtual domains.

If a chokepoint is not assigned to a map, you are not able to find that chokepoint using Search or Advanced Search.

All chokepoint setup is done using the AeroScout System Manager.

**Note**

See the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide* for configuration details at the following URL: <http://support.aeroscout.com>.

To monitor chokepoints, follow these steps:

- Step 1** Choose **Monitor > Chokepoints**. The Chokepoint page appears showing all mapped chokepoints.

Step 2 To refine the search criteria when an extensive list appears, search by MAC address or chokepoint name.

- a. To initiate a search for a chokepoint by its MAC address or chokepoint name, enter that value in the Search text box. Click **Search**.

This example show a search by MAC address.

If no match exists, a message appears in the Search Results page.

- b. To initiate an advanced search for a chokepoint by its MAC address or name, click the **Advanced Search** link.
 1. Choose **Chokepoint** as the search category.
 2. From the Search for Chokepoint by drop-down list, choose either **Chokepoint Name** or **MAC Address**.

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

3. Enter either the chokepoint name or MAC address.
4. Click **Search**.

This example shows an advanced search using the chokepoint name.

If no match exists, a message appears in the page. Otherwise the Search Results page appears.

Monitoring Wi-Fi TDOA Receivers

A Wi-Fi TDOA receiver must be assigned to a map for its location to be monitored. After adding the TDOA receiver to a map, you must resynchronize network designs (Services > Synchronize Services) with the mobility services engine for it to appear on the map.

If a TDOA receiver is not assigned to a map, you cannot find it using Search or Advanced Search.

All TDOA receiver setup is done using the AeroScout System Manager.

When a new TDOA receiver is created, it is available in all the virtual domains. After placing it on a floor, it is updated so that it is available in the same virtual domain as that of the floor. When a TDOA receiver is removed from a floor, it will be available in all the virtual domains again.

If the existing TDOA receivers are on a floor, then they all belong to the same virtual domain as the floor. If the chokepoints are not placed on a floor, then they are available in all virtual domains.



Note See the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide* for configuration details at the following URL: <http://support.aeroscout.com>.

To monitor TDOA receivers, follow these steps:

Step 1 Choose **Monitor > WiFi TDOA Receivers**. The WiFi TDOA Receivers summary page appears showing all mapped TDOA receivers.

Step 2 To refine the search criteria when an extensive list appears, search by MAC address or TDOA receiver name.

- a. To initiate a search for a TDOA receiver by its MAC address or name, enter that value in the Search text box. Click **Search**.
- b. Click **View List** to see a full list of alarms.

If no match exists, a message appears in the Search Results page.

- c. To initiate an advanced search for a TDOA receiver by its MAC address or name, click the **Advanced Search** link.
 1. Choose **WiFi TDOA Receiver** as the search category from the Search Criteria drop-down list.
 2. From the Search for WiFi TDOA Receiver by drop-down list, choose either **WiFi TDOA Receivers Name** or **MAC Address**.

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

3. Enter either the TDOA receiver name or MAC address.
4. Click **Search**.

This example shows an advanced search using the MAC address.

If no match exists, a message appears in the Search Results page.

Monitoring Geo-Location

The MSE provides physical location of wired clients, wired endpoints, switches, controllers, and access points present in a wireless network deployment. Currently, MSE provides location information in geo-location format to the external entities through northbound and southbound entities.

To improve the accuracy of the geo-location information provided by MSE, this feature aims to transform the geometric location co-ordinates of a device to geo-location coordinates (latitude and longitude) and provides it to the external entities through northbound and southbound interfaces.



Note

At least three GPS markers are required for geo-location calculation. The maximum number of GPS markers that you can add is 20.

This section contains the following topics:

- [Adding a GPS Marker to a Floor Map, page 11-60](#)
- [Editing a GPS Marker, page 11-60](#)
- [Deleting a GPS Marker Present on a Floor, page 11-61](#)

Adding a GPS Marker to a Floor Map

To add a GPS marker to a floor map, follow these steps:

-
- Step 1** Choose **Monitor > Site Maps** to display the Maps page.
- Step 2** Choose **Campus Name > Building Name > Floor Name**.
- Step 3** Choose the **Add/Edit GPS Markers Information** menu option on the top left menu to open the Add/Edit GPS page.
- A GPS Marker icon appears on the top left corner of the map (X=0 Y=0).
- Step 4** You can drag the GPS Marker icon and place it in the desired location on the map or enter the X and Y position values in the GPS Marker Details table on the left sidebar menu to move the marker to the desired position.
-  **Note** If the markers added are too close, then the accuracy of geo-location information is less.
-
- Step 5** Enter the Latitude and Longitude degrees for the selected GPS Marker icon in the left sidebar menu.
- Step 6** Click **Save**.
- The GPS Marker information is saved to the database.
- Step 7** Click **Apply to other Floors of Building** to copy GPS markers on one floor of a building to all the remaining floors of that building.
-

Editing a GPS Marker

To edit a GPS marker present on the floor, follow these steps:

-
- Step 1** Choose **Monitor > Site Maps** to display the Maps page.
- Step 2** Choose the **Campus Name > Building Name > Floor Name**.
- Step 3** Choose the **Add/Edit GPS Markers Information** menu option on the top left menu to open the Add/Edit GPS page.
- Step 4** Select an existing GPS marker present on the floor.
- Step 5** From the left sidebar menu, you can change the Latitude, Longitude, X Position, and Y Position which is associated with the GPS marker.
- Step 6** Click **Save**.
- The modified GPS marker information is now saved to the database.
-

Deleting a GPS Marker Present on a Floor

To delete a GPS marker present on a floor, follow these steps:

-
- Step 1** Choose **Monitor > Site Maps** to display the Maps page.
 - Step 2** Choose **Campus Name > Building Name > Floor Name**.
 - Step 3** Choose the **Add/Edit GPS Markers Information** menu option to open the Add/Edit GPS page.
 - Step 4** Select an existing GPS Marker which is present on the floor from the left sidebar menu.



Note You can delete multiple GPS markers present on a floor by selecting the **Multiple GPS Markers** check box.

- Step 5** Click **Delete GPS Marker**.
The selected GPS marker is deleted from the database.
-

Ekahau Site Survey Integration

Ekahau Site Survey (ESS) tool is used for designing, deploying, maintaining, and troubleshooting high performance Wi-Fi networks. ESS works over any 802.11 network and is optimized for centrally managed 802.11n Wi-Fi networks.

You can use the ESS tool to import the existing floor maps from the Prime Infrastructure and export the project to the Prime Infrastructure. For more information, see the Cisco Prime Infrastructure Integration section on the ESS online help or access the user guide at: C:\Program Files\Ekahaui\Ekahaui Site Survey\doc.



Note The Prime Infrastructure site survey calibration requires that you have collected at least 150 survey data points at 50 distinct locations. If you do not have enough survey data points, a warning is given when trying to export the survey data.



Note If there are no access points in the Prime Infrastructure during the site survey, the site survey will not happen.



Note If the floor map scales are incorrect in the Prime Infrastructure, the visualizations in the ESS will be distorted.

AirMagnet Survey and Planner Integration

AirMagnet survey and AirMagnet planner is integrated with the Cisco Prime Infrastructure. This integration increases the operational efficiencies by eliminating the need to repeat the wireless planning and site survey tasks commonly associated with deployment and management of wireless LAN networks.

The AirMagnet survey tool allows you to export real world survey data to the Prime Infrastructure for calibrating planner modelling. With the AirMagnet planner, you can create and export planner projects directly to the Prime Infrastructure. This enables the Prime Infrastructure to create its own project directly from the imported AirMagnet Planner tool. For more information, see AirMagnet Survey and Planning documentation.

Monitoring Wired Switches

You can review details on the wired switch (IP address, serial number, software version, and ELIN), its ports, its wired clients (count and status), and its civic information.

Wired switch data is downloaded to the mobility services engine through the Prime Infrastructure when the Ethernet switch and the mobility services engine are synchronized (Services > Synchronize Services > Switches). Communication between a location-capable switch and a mobility services engine occurs over NMSP. The Prime Infrastructure and the mobility services engine communicate over XML.

To view details on wired switches, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**.
 - Step 2** In the Mobility Services page, click the device name link of the appropriate wired location switch.
 - Step 3** Choose **Context Aware Service > Wired > Wired Switches**. A summary of wired switches that are synchronized with the mobility services engine appears.
 - Step 4** To see more details on the switch, its ports, its wired clients (count and status), and its civic information, click the **IP address** link.



Note You can export civic information from the switch by choosing that option from the Select a command drop-down list. This option is available on all four tabs in the Wired Switches page.

- On the Switch Information tab, a total count of wired clients connected to the switch is summarized along with their state (connected, disconnected, and unknown).
- Connected clients—Clients that are connected to the wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients are marked as unknown when the NMSP connection to the wired switch is lost.

You can view detailed wired client information by clicking one of the client count links (total clients, connected, disconnected, and unknown). See the [“Monitoring Wired Clients” section on page 11-63](#) for details.

- Step 5** Click the **Switch Ports** tab to see a detailed list of the ports on the switch.

You can change the listing order (ascending, descending) of port IP addresses, slot numbers, module number, and port number by clicking the respective column heading.

- Step 6** Click the **Civic** tab to see a detailed list of the civic information for the wired switch.
- Step 7** Click the **Advanced** tab to see a detailed list of the additional civic information for the wired switch.
-

Monitoring Wired Clients

You can view details on a wired client (MAC address, IP address, username, serial number, UDI, model no., software version, and VLAN ID), its port, and its civic information.

Wired client data is downloaded to the mobility services engine through the Prime Infrastructure when the switch and the mobility services engine are synchronized (Services > Synchronize Services > Switches).

Communication between a location-capable switch and a mobility services engine occurs over NMSP. The Prime Infrastructure and the mobility services engine communicate over XML.

You can view the details of the wired clients in either the Wired Switches page (Context Aware Service > Wired > Wired Switches) or wired clients page (Context Aware Service > Wired > Wired Clients).

- If you know the IP address, MAC address, VLAN ID, serial number, or username, you can use the Search text box in the Wired Clients page.
- If you want to examine wired clients as they relate to a specific switch, you can view that information in the Wired Switches page. See the [“Monitoring Wired Clients” section on page 11-63](#).

To view details on a wired client, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**. The Mobility Services page appears.
- Step 2** Click the device name link of the appropriate wired location switch.
- Step 3** Choose **Context Aware Service > Wired > Wired Clients**.

In the Wired Clients summary page, clients are grouped by their switch.

The status of a client is noted as connected, disconnected, or unknown. Definitions are summarized as follows:

- Connected clients—Clients that are active and connected to a wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the NMSP connection to the wired switch is lost.
- If you know the MAC address of the wired client, then you can click that link to reach the detail page of the client or use the Search text box.
 - You can also search for a wired client by its IP address, username, or VLAN ID.
- If you click the IP address of the switch, you are forwarded to the detail page of the switch. See the [“Monitoring Wired Clients” section on page 11-63](#).

- Step 4** Click the **Port Association** tab to show the physical location of the switch port/slot/module on which the wired client terminates, the client status (connected, disconnected, unknown), and the switch IP address.
- Step 5** Click the **Civic Address** tab to show any civic address information.
- Step 6** Click the **Advanced** tab to see extended physical address details for the wired clients, if any.

**Note**

A client takes on the civic address and advanced location information that is configured for the port on which the client terminates. If no civic and advanced information are defined for the port (port/slot/module), then no location data is displayed.

Monitoring Interferers

The Monitor > Interferer page allows you to monitor interfering devices detected by the CleanAir-enabled access points.

This section contains the following topics:

- [Monitor > Interferers > AP Detected Interferers](#), page 11-64
- [Monitor > Interferers > AP Detected Interferers > Interferer Details](#), page 11-65
- [Monitor > Interferers > Edit View](#), page 11-67
- [Clustering of Monitor Mode APs Using the MSE](#), page 11-69

Monitor > Interferers > AP Detected Interferers

Choose **Monitor > Interferers** to view all the interfering devices detected by the CleanAir-enabled access points on your wireless network. This page enables you to view a summary of the interfering devices including the following default information:

**Note**

Whenever an Inverter or a Jammers is detected on your network, an alarm is generated and the same information is displayed on the Security Dashboard of the Prime Infrastructure UI. The controller sends traps to the Prime Infrastructure for the corresponding device.

- Interferer ID—A unique identifier for the interferer. Click this link to learn more about the interferer.
- Type—Indicates the category of the interferer. Click to read more about the type of device. The pop-up dialog appears displaying more details. The categories include the following:
 - Bluetooth link—A Bluetooth link (802.11b/g/n only)
 - Microwave Oven—A microwave oven (802.11b/g/n only)
 - 802.11 FH—An 802.11 frequency-hopping device (802.11b/g/n only)
 - Bluetooth Discovery—A Bluetooth discovery (802.11b/g/n only)
 - TDD Transmitter—A time division duplex (TDD) transmitter
 - Jammer—A jamming device
 - Continuous Transmitter—A continuous transmitter
 - DECT-like Phone—A Digital Enhanced Cordless Telecommunication (DECT)-compatible phone
 - Video—A video camera
 - 802.15.4—An 802.15.4 device (802.11b/g/n only)

- WiFi Inverted—A device using spectrally inverted Wi-Fi signals
- WiFi Invalid—A device using non-standard Wi-Fi channels
- SuperAG—An 802.11 SuperAG device
- Canopy—A Motorola Canopy device
- Radar—A radar device (802.11a/n only)
- Xbox—A Microsoft Xbox (802.11b/g/n only)
- WiMAX Mobile—A WiMAX mobile device (802.11a/n only)
- WiMAX Fixed—A WiMAX fixed device (802.11a/n only)
- Status—Indicates the status of the interfering device.
 - Active—Indicates that the interferer is currently being detected by the CleanAir-enabled access point.
 - Inactive—Indicates that the interferer is no longer being detected by the CleanAir-enabled access point or the CleanAir-enabled access point detected that the interferer is no longer reachable by the Prime Infrastructure.
- Severity—Shows the severity ranking of the interfering device.
- Affected Band—Shows the band in which this device is interfering.
- Affected Channels—Shows the affected channels.
- Duty Cycle (%)—The duty cycle of interfering device in percentage.
- Discovered—Shows the time at which it was discovered.
- Last Updated—The last time the interference was detected.
- Floor—The location where the interfering device is present.

**Note**

These devices appear only if the option to track Interferers is enabled in the Tracking Parameters page. This option is disabled by default. For more information on tracking parameters, see the [“Modifying Tracking Parameters” section on page 9-22](#).

Monitor > Interferers > AP Detected Interferers > Interferer Details

Choose **Monitor > Interferers > Interferer ID** to view this page. This page enables you to view the details of the interfering devices detected by the access points. This page provides the following details about the interfering device:

- Interferer Properties
 - Type—Shows the type of the interfering device detected by the AP.
- Status—The status of the interfering device.
 - Active—Indicates that the interferer is currently being detected by the CleanAir-enabled access point.
 - Inactive—Indicates that the interferer is no longer being detected by the CleanAir-enabled access point or the CleanAir-enabled access point detected that the interferer is no longer reachable by the Prime Infrastructure.
 - Severity—Shows the severity ranking of the interfering device.

- Duty Cycle (%)—The duty cycle of interfering device in percentage.
- Affected Band—Shows the band in which this device is interfering.
- Affected Channels—Shows the affected channels.
- Discovered—Shows the time at which it was discovered.
- Last Updated—The last time the interference was detected.
- Location
 - Floor—The location where this interfering device was detected.
 - Last Located At—The last time where the interfering device was located.
 - On MSE—The mobility services engine on which this interfering device was located.
- Clustering Information
 - Clustered By—Shows the following:
 - IP address of the controller if clustered by a controller.
 - IP address of the mobility services engine if clustered by a mobility services engine.
 - Detecting APs—Shows the details of the access point that has detected the interfering device. The details include Access Point Name (MAC), Severity, and Duty Cycle(%).

**Note**

The detecting access point information is available only for active devices and sometimes information about the active devices may not be available. This is because interferers are in the process of being marked inactive and in the next refresh of the Monitor > Interferers page, appear as inactive.

- Details—Shows a short description about the interfering type.

Select a command

The Select a command drop-down list provides access to the location history of the interfering device detected by the access point. See the [“Monitor > Interferers > AP Detected Interferer Details > Interference Device ID > Location History”](#) section on page 11-66.

Monitor > Interferers > AP Detected Interferer Details > Interference Device ID > Location History

Choose **Monitor > Interferers > Interference Device ID**, choose **Location History** from the Select a command drop-down list, and click **Go** to view this page.

- Interferer Information—Displays the basic information about the interfering device.
 - Data Collected At—The time stamp at which the data was collected.
 - Type—The type of the interfering device.
 - Severity—The severity index of the interfering device.
 - Duty Cycle—The duty cycle (in percentage) of the interfering device.
 - Affected Channels—A comma-separated list of the channels affected.
- Interferer Location History—Displays the location history of the interfering devices.

- Time Stamp
- Floor
- Clustering Information
 - Clustered By
- Detecting APs
 - AP Name—The access point that detected the interfering device.
 - Severity—The severity index of the interfering device.
 - Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.
- Location
 - Location Calculated At—Displays the time stamp at which this information was generated.
 - Floor—Displays location information of the interfering device.
 - A graphical view of the location of the interfering device is displayed in a map. Click the **Enlarge** link to view an enlarged image.

Monitor > Interferers > Edit View

The Edit View page allows you to add, remove, or reorder columns in the AP Detected Interferers Summary page. It also allows you to search for Interferers. By default, only those interferers that are in Active state and with a severity greater than or equal to 5 are displayed in the AP Detected Interferers page. For more information on editing search criteria, see the “[Monitor > Interferers > Edit View > Edit Search](#)” section on page 11-67.

To edit the columns in the AP Detected Interferers page, follow these steps:

-
- Step 1** Choose **Monitor > Interferers**. The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir-enabled access points.
 - Step 2** Click the **Edit View** link in the AP Detected Interferers page.
 - Step 3** To add an additional column to the access points table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the table.
 - Step 4** To remove a column from the access points table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. All items in the left column are not displayed in the table.
 - Step 5** Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.
 - Step 6** Click **Reset** to restore the default view.
 - Step 7** Click **Submit** to confirm the changes.
-

Monitor > Interferers > Edit View > Edit Search

You can search for interferers based on certain criteria. By default, only those interferers that are in Active state and with a severity greater than or equal to 5 are displayed in the AP Detected Interferers page. Use the Edit Search option to customize the interferer search.

To edit the search criteria, follow these steps:

- Step 1** Choose **Monitor > Interferers**. The AP Detected Interferers page appears.
- Step 2** Click **Edit Search** and complete the applicable parameters in the New Search dialog box (see [Figure 11-8](#)).

Figure 11-8 *Monitor > Interferers > Edit View > Edit Search*

The screenshot shows a 'New Search' dialog box with the following fields and values:

- Search Category: Interferers
- Detected By: Access Points
- Search By: Severity
- Severity greater than: 5
- Detected within the last: All History
- Interferer Status: Active
- Restrict By Radio Band/Channels:
- Items per page: 50
- Save Search:

This option allows you to specify the following search criteria:

- Search Category—For interferer search, the search category is Interferers.
- Detected By—Choose from the drop-down list if the interferer is detected by access points or interferer.
- Search By—Choose one of the options from the list:
 - All Interferers
 - Interferer ID
 - Interferer Type
 - Severity
 - Duty Cycle
 - Location
- Severity greater than—Enter the severity level in the text box.
- Detected within the last—Choose one of the following option from the drop-down list:
 - 5 Minutes
 - 15 Minutes
 - 30 Minutes
 - 1 Hour
 - 3 Hours
 - 6 Hours
 - 12 Hours
 - 24 Hours
 - All History
- Interferer status—Choose one of the following option from the drop-down list:

- **Active**
 - **Inactive**
 - **All**
 - **Restrict By Radio Band/Channels**—Select this check box if you want to restrict certain radio frequencies or channels from the search. By default, this check box is unselected. On selecting this check box, a drop-down list appears with 2.4-GHz, 5-GHz and Individual Channel options. If you choose Individual Channel, an Affected Channels text box appears. Specify the channel and select either the **Match All** or **Match Any** radio button.
- Step 3** Select the number of items per page that you want to view in the search results.
- Step 4** Select the **Save Search** check box if you want to save the search.
- Step 5** After specifying the search criteria, click **Go** to view the search results.
-

Clustering of Monitor Mode APs Using the MSE

You can use the MSE to cluster monitor-mode APs for interference detection and location process. This clustering is based on distance and not neighbor maps. All Monitor mode APs within 150 feet from a particular AP form a cluster.

However, this fixed distance does not work for some of the scenarios and needs to be configured. You can use the following command to change the default distance value for clustering:

```
config spectrum-monitor-mode-ap-clustering-distance value
```

Where *value* is the distance in feet for clustering. The default value is 150.



CHAPTER 12

MSAP

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

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



Note

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

This chapter contains the following sections:

- [Licensing for MSAP, page 12-1](#)
- [Provisioning MSAP Service Advertisements, page 12-2](#)
- [Deleting Service Advertisements, page 12-4](#)
- [Applying Service Advertisements to a Venue, page 12-4](#)
- [Viewing the Configured Service Advertisements per MSE, page 12-5](#)
- [Viewing MSAP Statistics, page 12-5](#)
- [Viewing the MSE Summary Page for MSAP License Information, page 12-6](#)
- [Viewing Service Advertisements Synchronization Status, page 12-6](#)
- [MSAP Reports, page 12-6](#)

Licensing for MSAP

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

Provisioning MSAP Service Advertisements

To add new MSAP advertisements, follow these steps:



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

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

Adding Venue Policy to Service Advertisements



Note You can also apply service advertisements to a venue by choosing **Services > MASP**. See the [“Applying Service Advertisements to a Venue”](#) section on page 12-4 for more information on how to apply service advertisements.

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



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

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

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

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

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

- **Radio**—Select the radio frequency on which you want the advertisements to be broadcasted. The service advertisement is displayed when the mobile device is near the radio band that you have selected. The possible values are 2.4 GHz or 5 GHz.
- **min RSSI**—Enter a value for RSSI at which you want the service advertisements to be displayed on the user interface.

Step 14 Click **Save** to add the venue. The venue is added to the list of venues in the Service Advertisement Details page.

Adding Service Brief Information to the Service Advertisement

Step 15 Click **Add Advertisement**.

The Add/Edit Advertisement page appears.

Step 16 From the Advertisement Type drop-down list, choose the type of advertisement you want to display.

Step 17 Enter the name that you want to display on the handset in the Friendly Name text box.

Step 18 Enter the service description in the Friendly Description text box.

Step 19 Enter the URL for each type of handset. The URL identifies the location at which the service can be retrieved. You can add multiple URLs by clicking **Add More URL**.

Step 20 Click **Save**. This information is applied to the MSE and the synchronization happens automatically.

Adding Service Advertisements to the Floor Map

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

Step 1 Choose Monitor > Site Maps.

The Site Maps page is displayed.

Step 2 Choose the appropriate floor location link from the list.

A map appears showing the placement of all installed access points, client, and tags and their relative signal strength.

Step 3 Click on Services icon on the floor map page.

The Venue dialog box to associate service advertisement to that particular venue is displayed.

Step 4 Click on Show/Associate Services link to open the Add/Edit MSAP Services.

The list of all the available service advertisements are displayed and you can associate service advertisements by selecting them.

Step 5 To associate a service advertisement, you can do the following:

- You can select an advertisement by filtering based on either provider name or friendly name by selecting them from the Filter By drop down list.
- or
- You can click on Associate check box to associate that particular service advertisement.

Step 6 Click OK.

Creating Service Advertisements from the Floor Map

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

-
- Step 1** Choose Monitor > Site Maps.
The Site Maps page is displayed.
 - Step 2** Choose the appropriate floor location link from the list.
A map appears showing the placement of all installed access points, client, and tags and their relative signal strength.
 - Step 3** Click on Services icon on the floor map page.
The Venue dialog box to associate service advertisement to that particular venue is displayed.
 - Step 4** Click on Show/Associate Services link to open the Add/Edit MSAP Services.
The list of all the available service advertisements are displayed and you can associate service advertisements by selecting them.
 - Step 5** Click Create MSAP Service to create service advertisements.
It redirects you to Service > MSAP > Add Service Advertisements page.
 - Step 6** Follow steps given in [Provisioning MSAP Service Advertisements, page 12-2](#) to create service advertisements.
-

Deleting Service Advertisements

To delete a service advertisement, follow these steps:

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

Applying Service Advertisements to a Venue

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

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

- Step 5** Follow [Step 6](#) through [Step 14](#) in the “[Provisioning MSAP Service Advertisements](#)” section on [page 12-2](#).
- or
- Click **Apply to Venues** in the MSAP page and follow [Step 6](#) through [Step 14](#) in the “[Provisioning MSAP Service Advertisements](#)” section on [page 12-2](#).
-

Viewing the Configured Service Advertisements per MSE

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

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

Viewing MSAP Statistics

To view MSAP statistics, follow these steps:

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

Viewing the MSE Summary Page for MSAP License Information

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

Viewing Service Advertisements Synchronization Status

To view service advertisements synchronization status, follow these steps:

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

MSAP Reports

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

- [Mobile MAC Statistics, page 12-6](#)
- [Service URI Statistics, page 12-7](#)

Mobile MAC Statistics

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

To create a new report, click **New** in the Report Launch Pad page or in the Mobile MAC Statistics Reports page. See the “[Configuring a Mobile MAC Statistics Report](#)” section on [page 12-6](#) for more information.

Configuring a Mobile MAC Statistics Report

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

Settings

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

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



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

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



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



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

The Mobile MAC Statistics report results contain the following:

- Mobile MAC
- Click Count



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

Service URI Statistics

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

To create a new report, click **New** from the Report Launch Pad or from the Mobile MAC Statistics Reports page. See the [“Configuring a Service URI Statistics Report”](#) section on page 12-7 for more information.

Configuring a Service URI Statistics Report

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

Settings

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

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



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

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



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



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

The Service URI Statistics report results contain the following:

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



CHAPTER 13

Performing Maintenance Operations

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

This chapter contains the following sections:

- [Guidelines and Limitations, page 13-1](#)
- [Recovering a Lost Password, page 13-1](#)
- [Recovering a Lost Root Password, page 13-2](#)
- [Backing Up and Restoring Mobility Services Engine Data, page 13-2](#)
- [Downloading Software to the Mobility Services Engines, page 13-4](#)
- [Configuring the NTP Server, page 13-6](#)
- [Resetting the System, page 13-6](#)
- [Clearing the Configuration File, page 13-7](#)

Guidelines and Limitations

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

Recovering a Lost Password

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

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

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

Recovering a Lost Root Password

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

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



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

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



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

Backing Up and Restoring Mobility Services Engine Data

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

This section contains the following topics:

- [Guidelines and Limitations, page 13-2](#)
- [Backing Up Mobility Services Engine Historical Data, page 13-3](#)
- [Restoring Mobility Services Engine Historical Data, page 13-3](#)
- [Enabling Automatic Location Data Backup, page 13-4](#)

Guidelines and Limitations

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

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

Backing Up Mobility Services Engine Historical Data

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

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

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

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



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



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

Restoring Mobility Services Engine Historical Data

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

To restore mobility services engine data, follow these steps:

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

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

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



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

Enabling Automatic Location Data Backup

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

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

Downloading Software to the Mobility Services Engines

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

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

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



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

Manually Downloading Software

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

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



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



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

Your entries should look like the following example:

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

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

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

Step 2 Manually stop the mobility services engine.

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

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

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

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

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

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



Caution

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

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

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

Configuring the NTP Server

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



Note

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

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

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



Note

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

Resetting the System

For information on rebooting or shutting down the mobility services engine hardware, see the “Rebooting or Shutting Down a System” section on page 6-9.

Clearing the Configuration File

For information on clearing the configuration file, see the [“Clearing the System Database”](#) section on page 6-9.



APPENDIX **A**

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. This 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 A-1](#)
- [Certificate Management, page A-2](#)
- [Prime Infrastructure GUI Updates for SNMPv3, page A-10](#)
- [Updated Open Port List, page A-10](#)
- [Syslog Support, page A-10](#)
- [MSE and RHEL 5, page A-11](#)

Setup Wizard Update

This section describes the configuration options that have been included in the Setup.sh script and contains the following topics:

- [Configuring Future Restart Day and Time, page A-1](#)
- [Configuring the Remote Syslog Server to Publish MSE Logs, page A-2](#)
- [Configuring the Host Access Control Settings, page A-2](#)

Configuring 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 the default.

Example:

```
Configure future restart day and time ? (Y)es/(S)kip [Skip]:
```

Configuring the 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:

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
```

Configuring the Host Access Control Settings

You can use this option to add, 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 (Rewrite the IP)
```

For more information on the setup.sh script, see the *Cisco 3350 Mobility Services Engine Getting Started Guide*.

Certificate Management

Currently, MSE ships with self-generated certificates. For establishing the trust in an 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 command-line interface 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/
```

This section describes the tasks you can perform using the CertMgmt.sh script and contains the following topics:

- [Creating a CSR, page A-3](#)
- [Importing the CA Certificate, page A-4](#)
- [Importing the Server Certificate, page A-4](#)
- [Enabling or Disabling Client Certificate Validation, page A-5](#)
- [Configuring OCSP Settings, page A-5](#)
- [Importing a CRL, page A-6](#)
- [Clearing Certificate Configuration, page A-6](#)
- [Showing Certificate Configuration, page A-7](#)

Creating 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 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/mserverkey.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/mservercsr.pem
The Private key is in: /root/TestFolder/mserverkey.pem

```

Importing the 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

```

Importing the 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
```

Enabling or Disabling 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: OCSF 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: OCSF 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
```

Configuring OCSF Settings

Use this option to configure the Online Certificate Status Protocol (OCSF) settings. You are prompted to enter the OCSF 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

```

Importing a CRL

Use this option to import a certificate revocation list (CRL) which you 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

```

Clearing Certificate Configuration

Use this option to clear the certificate configuration.

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 ]

```

Showing Certificate Configuration

Use this option to display the certificate configuration 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:fl:

```

```

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
***** OCSF Setting *****
OCSP URL :
http://ocsp.227.104.178.224
OCSP nick name :ExampleServer
=====

```

Prime Infrastructure GUI Updates for SNMPv3

For more information on SNMPv3-related graphical user interface changes, see the following sections:

- [Adding an Event Definition, page 8-8](#)
- [Adding Trap Destinations, page 6-5](#)

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 ports for MSE:

TCP	80, 443, 22, 8001
	4096, 1411, 4000X (x=1,5)
UDP	162, 12091, 12092

Syslog Support

To ensure compliance with DoD requirements, 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

Numerics

802.1n scaling reports [11-9](#)

A

access points, adding to maps [10-11 to 10-14](#)

adding [7-1, 7-3, 8-7, 8-8](#)

alarm notifications

 emailing [11-5](#)

applying calibration models [9-3](#)

assigning location presence [10-3, 11-50](#)

audit report

 for alarms [11-4](#)

automatic backup [13-4](#)

automatic synchronization [3-6](#)

B

backup historical data [13-3](#)

buildings

 adding to NCS database [10-4, 11-50](#)

C

certificate management [A-2](#)

change order buttons [11-14](#)

civic address [10-4, 11-50](#)

clear [11-5](#)

color coding

 of obstacles [10-20](#)

configuring [11-7, 13-6](#)

ContextAware tab [1-3](#)

Current building

 delete [11-52](#)

 edit map [11-52](#)

customize report [11-14](#)

D

deleting [7-2, 7-3, 8-7, 8-12](#)

destination type

 for report [11-11](#)

download [11-8](#)

drawing polygon areas

 using map editor [10-19](#)

E

edited saved marker [11-17](#)

editing [6-1](#)

editing scheduled run details [11-16](#)

edit location presence information [10-3, 11-50](#)

event history [11-4](#)

F

failover [4-2](#)

filtering scheduled run results [11-16](#)

G

general properties [6-1](#)

H

heat map

described [10-13](#)

high availability [4-1](#)

history parameters editing [9-28](#)

http

//support.aeroscout.com [11-58](#)

I

identity client [11-47](#)

L

licensing for MSAP [12-1](#)

location presence

assigning [10-3](#), [11-50](#)

location smoothing [9-32](#)

M

managing current reports [11-15](#)

managing saved reports [11-16](#)

map editor

using to draw polygon areas [10-19](#)

MSAP [12-1](#)

MSAP provisioning [12-2](#)

MSAP reports [12-6](#)

N

network designs [3-1](#)

NTP Server

Configuring [13-6](#)

O

onstacole color coding [10-20](#)

out-of-sync [3-7](#)

P

pairing matrix [4-2](#)

permission [7-2](#)

placement of access points [10-14](#)

polling parameters

editing [9-22](#), [9-26](#)

properties [7-4](#)

pull [1-6](#)

R

recovering lost [13-1](#)

recurrence

for report [11-11](#)

report launch pad [11-9](#)

restore historical data [13-3](#)

RFID Asset Tags [1-3](#)

rogue access points [1-3](#)

running new [11-9](#)

S

scheduled runs [11-15](#)

scheduled tasks [3-6](#)

service advertisements [12-4](#)

service advertisement synchronization [12-6](#)

set sorting buttons [11-14](#)

Simple Mail Transfer Protocol [1-5](#)

Simple Network Management Protocol [1-5](#)

SMTP [1-5](#)

SNMP [1-5](#)

SOAP [1-5](#)

software download [13-4](#)
Specifies Simple Object Access Protocol [1-5](#)
Standalone Building
 adding floor plan [10-8](#)
statistics [9-37](#)
summary [8-12](#)
synchronization [3-7](#)
synchronization history [3-8](#)
SysLog [1-5](#)
system and appliance hardening [A-1](#)

T

testing [8-12](#)
tracking parameters [9-22](#)

U

using planning mode [10-19](#)

V

viewing [11-2, 11-6](#)
viewing HA parameters [4-6](#)
viewing HA status [4-7](#)
viewing MSAP statistics [12-5](#)

