



Cisco Connected Mobile Experiences Configuration Guide, Release 7.6

First Published: July 31, 2013

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-29330-01

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

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

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 NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

Cisco 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: <http://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)

© 2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface xv

Audience xv

Related Documentation xv

Obtaining Documentation and Submitting a Service Request xv

CHAPTER 1

Overview 1

About the Cisco Context-Aware Mobility Solution 1

Cisco 3300 Series Mobility Services Engine 1

Context-Aware Service (CAS) 2

ContextAware Tab 2

Licensing Information for Clients and Tags 3

Viewing Contextual Information 3

Location Assisted Client Troubleshooting from the ContextAware Dashboard 4

Event Notification 4

CHAPTER 2

Adding and Deleting Mobility Services Engines and Licenses 7

Licensing Requirements for MSE 7

MSE License Structure Matrix 8

Sample MSE License File 8

Revoking and Reusing an MSE License 9

Guidelines and Limitations 9

Adding a Mobility Services Engine to the Prime Infrastructure 9

Enabling Services on the Mobility Services Engine 11

Configuring MSE Tracking and History Parameters 12

Assigning Maps to the MSE 13

Deleting an MSE License File 14

Deleting a Mobility Services Engine from the Prime Infrastructure 14

Registering Device and wIPS Product Authorization Keys 14

Installing Device and wIPS License Files 15

CHAPTER 3

Synchronizing Mobility Services Engines 17

Synchronizing the Prime Infrastructure and Mobility Services Engines 17

Prerequisites for Synchronizing Mobility Services Engine 18

Working with Third-Party Elements 18

 Deleting the Elements or Marking Them as Third-Party Elements 19

Synchronizing Cisco WLC with a Mobility Services Engine 19

 Assigning and Synchronizing Network Designs, a Cisco WLC, Catalyst Switch, or Event Group 19

 Assigning an MSE to the Cisco WLC 20

 Unassigning a Network Design, Wired Switch, or Event Group from MSE 21

Configuring Automatic Database Synchronization and Out-of-Sync Alerts 21

 Configuring Automatic Database Synchronization 22

 Smart Controller Assignment and Selection Scenarios 22

 Out-of-Sync Alarms 23

Viewing the Status of Mobility Services Engine Synchronization 23

 Viewing the Status of Mobility Services Engine Synchronization 24

 Viewing Synchronization History 24

CHAPTER 4

Configuring High Availability 27

Overview of the High Availability Architecture 27

Pairing Matrix 28

Guidelines and Limitations for High Availability 28

Failover Scenario for High Availability 29

Failback Scenario for High Availability 29

HA Licensing 29

Configuring High Availability on the MSE 29

Viewing Configured Parameters for High Availability 43

Viewing High Availability Status 43

CHAPTER 5

MSE Delivery Modes 45

Physical Appliance 45

Virtual Appliance 45

Viewing the MSE License Information Using the License Center 46

Removing a License File Using the License Center 47

CHAPTER 6**Configuring and Viewing System Properties 49**

Licensing Requirement 49

Editing General Properties and Viewing Performance 49

Editing General Properties 50

Viewing Performance Information 52

Modifying NMSP Parameters 52

Viewing Active Sessions on a System 54

Adding and Deleting Trap Destinations 54

Adding Trap Destinations 55

Deleting Trap Destinations 56

Viewing and Configuring Advanced Parameters 56

Viewing Advanced Parameter Settings 57

Initiating Advanced Parameters 57

Configuring Advanced Parameters 58

Initiating Advanced Commands 59

Rebooting or Shutting Down a System 59

Clearing the System Database 59

CHAPTER 7**Mobile Concierge Services 61**

Licensing for Mobile Concierge 61

Defining a Venue 62

Deleting the Venue 63

Adding New Service Providers with Policies 63

Adding New Service Providers with Policies 64

Deleting a Service Provider 65

Defining New Policies 65

Deleting Policies 66

CHAPTER 8**Managing Users and Groups 67**

Prerequisites 67

Guidelines and Limitations 67

Managing User Groups 67

Adding User Groups	67
Deleting User Groups	68
Changing User Group Permissions	68
Managing Users	69
Adding Users	69
Deleting Users	70
Changing User Properties	70

CHAPTER 9**Configuring Event Notifications 71**

Information About Event Notifications	71
Viewing Event Notification Summary	72
Clearing Notifications	72
Notification Message Formats	73
Notification Formats in Text	73
Notification Formats in XML	73
Missing (Absence) Condition	74
In/Out (Containment) Condition	74
Distance Condition	75
Battery Level	75
Location Change	75
Chokepoint Condition	75
Emergency Condition	75
Adding and Deleting Event Groups	76
Adding Event Groups	76
Deleting Event Groups	76
Adding, Deleting, and Testing event Definitions	77
Adding an Event Definition	77
Deleting an Event Definition	79
Testing Event Definitions	79
Prime Infrastructure as a Notification Listener	80

CHAPTER 10**Context-Aware Service Planning and Verification 81**

Licensing Requirement	81
Planning Data, Voice, and Location Deployment	81
Guidelines and Limitations	82

Calculating the Placement of Access Points	82
Calibration Models	83
Guidelines and Limitations for Calibration Model	83
Creating and Applying Data Point and Calibration Models	83
Inspecting Location Readiness and Quality	85
Guidelines and Limitations	86
Inspecting Location Readiness Using Access Point Data	86
Inspecting Location Quality Using Calibration Data	86
Verifying Location Accuracy	87
Using Scheduled Accuracy Testing to Verify Current Location Accuracy	87
Using On-Demand Location Accuracy Testing	88
Using Optimized Monitor Mode to Enhance Tag Location Reporting	90
Guidelines and Limitations	90
Optimizing Monitoring and Location Calculation of Tags	90
Configuring Interferer Notification	91
Modifying Context-Aware Service Parameters	92
Licensing Requirement	92
Guidelines and Limitations	92
Modifying Tracking Parameters	92
Guidelines and Limitations	93
Configuring Tracking Parameters for a Mobility Services Engine	93
Modifying Filtering Parameters	96
Guidelines and Limitations	97
Configuring Filtering Parameters for a Mobility Services Engine	97
Modifying History Parameters	98
Guidelines and Limitations	99
Configuring Mobility Services Engine History Parameters	99
Enabling Location Presence	100
Guidelines and Limitations	100
Enabling and Configuring Location Presence on a Mobility Services Engine	100
Importing and Exporting Asset Information	101
Importing Asset Information	101
Exporting Asset Information	102
Modifying Location Parameters	102
Configuring Location Parameters	102

Enabling Notifications and Configuring Notification Parameters	105
Enabling Notifications	105
Configuring Notification Parameters	105
Viewing Notification Statistics	107
Location Template for Cisco Wireless LAN Controllers	108
FastLocate Overview	109
Configuring a New Location Template for a Wireless LAN Controller	110
Location Services on Wired Switches and Wired Clients	111
Prerequisites to Support Location Services for Wired Clients	111
Guidelines and Limitations	112
Configuring a Catalyst Switch Using the CLI	112
Adding a Catalyst Switch to Prime Infrastructure	114
Assigning and Synchronizing a Catalyst Switch to a Mobility Services Engine	114
Verifying an NMSP Connection to a Mobility Services Engine	115

CHAPTER 11
Working with Maps 117

About Maps	117
Adding a Building to a Campus Map	118
Adding Floor Areas	119
Adding Floor Areas to a Campus Building	119
Adding Floor Plans to a Standalone Building	121
Adding a Campus Map	123
Configuring Buildings	123
Adding a Building to a Campus Map	124
Adding a Standalone Building	125
Viewing a Building	126
Editing a Building	127
Deleting a Building	127
Moving a Building	128
Adding Floor Areas	128
Adding Floor Areas to a Campus Building	128
Adding Floor Plans to a Standalone Building	130
Configuring Floor Settings	132
Defining Inclusion and Exclusion Regions on a Floor	133
Cisco 1000 Series Lightweight Access Point Icons	133

Filtering Access Point Floor Settings	136
Filtering Access Point Heatmap Floor Settings	138
Filtering AP Mesh Info Floor Settings	139
Filtering Client Floor Settings	140
Filtering 802.11 Tag Floor Settings	141
Filtering Rogue AP Floor Settings	141
Filtering Rogue Adhoc Floor Settings	142
Filtering Rogue Client Floor Settings	142
Filtering Interferer Settings	143
Filtering wIPS Attacker Floor Settings	143
Import Map and AP Location Data	145
Monitoring the Floor Area	146
Planning and Zooming with Next Generation Maps	146
Adding Access Points to a Floor Area	147
Placing Access Points	148
Using the Automatic Hierarchy to Create Maps	149
Using the Map Editor	152
Guidelines for Using the Map Editor	152
Guidelines for Inclusion and Exclusion Areas on a Floor	153
Opening the Map Editor	153
Using the Map Editor to Draw Coverage Areas	153
Defining an Inclusion Region on a Floor	154
Defining an Exclusion Region on a Floor	155
Defining a Rail Line on a Floor	155
Adding an Outdoor Area	156
Using Planning Mode	157
Using Chokepoints to Enhance Tag Location Reporting	158
Adding Chokepoints to the Prime Infrastructure	159
Adding a Chokepoint to a Prime Infrastructure Map	159
Removing Chokepoints from the Prime Infrastructure	160

CHAPTER 12
Monitoring the System and Services 161

Working with Alarms	162
Guidelines and Limitations	162
Viewing Alarms	162

Monitoring Cisco Adaptive wIPS Alarm Details	163
Assigning and Unassigning Alarms	165
Deleting and Clearing Alarms	165
E-mailing Alarm Notifications	165
Working with Events	166
Displaying Location Notification Events	166
Working with Logs	167
Guidelines and Limitations	167
Configuring Logging Options	167
MAC address-based Logging	168
Downloading Log Files	168
Generating Reports	169
Report Launch Pad	169
Creating and Running a New Report	170
Managing Current Reports	175
Managing Scheduled Run Results	175
Sorting Scheduled Run Results	175
Viewing or Editing Scheduled Run Details	176
Managing Saved Reports	176
Sorting Saved Reports	177
Viewing or Editing Saved Report Details	177
Generating MSE Analytics Reports	178
Associated vs. Probing Clients by Selected Zone	178
Client Location	178
Configuring a Client Location History Report	179
Client Location Results	180
Client Location Density	180
Configuring a Client Location Density Report	180
Client Location Density Results	182
Device Count by Zone	182
Configuring a Device Dwell by Zone Report	182
Device Count by Zone Results	183
Device Dwell Time by Zone	184
Configuring a Device Dwell by Zone Report	184
Device Count by Zone Results	185

Guest Location Density	185
Configuring Guest Location Density	185
Guest Location Density Results	186
Location Notifications by Zone	187
Configuring a Location Notification Report	187
Location Notification Results	188
Mobile MAC Statistics	188
Configuring Mobile MAC Statistics	188
Mobile MAC Tracking Results	189
Rogue AP Location Density	190
Configuring Rogue AP Location Density	190
Rogue Client Location Density	191
Configuring Rogue Client Location Density	191
Rogue Client Location Tracking Results	192
Tag Location Tracking	193
Configuring Tag Location Tracking	193
Tag Location Tracking Results	194
Creating a Device Utilization Report	195
Viewing Saved Utilization Reports	197
Viewing Scheduled Utilization Runs	197
Managing OUI	197
Adding a New Vendor OUI Mapping	197
Uploading an Updated Vendor OUI Mapping File	198
Monitoring Wireless Clients	198
Monitoring Wireless Clients Using Maps	199
Monitoring Wireless Clients Using Search	201
Client Support on the MSE	202
Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address	202
Viewing the Clients Detected by the MSE	203
Configuring Buildings	209
Adding a Building to a Campus Map	209
Adding a Standalone Building	211
Viewing a Building	212
Editing a Building	212
Deleting a Building	213

Moving a Building	213
Monitoring Tags	213
Monitoring Tags Using Maps	214
Monitoring Tags Using Search	214
Overlapping Tags	216
Monitoring Geo-Location	217
Adding a GPS Marker to a Floor Map	217
Editing a GPS Marker	218
Deleting a GPS Marker From the Floor	218
Monitoring Chokepoints	218
Monitoring Wi-Fi TDOA Receivers	219
Ekahau Site Survey Integration	220
AirMagnet Survey and Planner Integration	221
Monitoring Wired Clients	221
Monitoring Wired Switches	222
Monitoring Interferers	223
Monitor > Interferers > AP Detected Interferers	223
Monitor > Interferers > Edit View	224
Clustering of Monitor Mode APs Using MSE	225

CHAPTER 13

Performing Maintenance Operations	227
Guidelines and Limitations	227
Recovering a Lost Password	227
Recovering a Lost Root Password	228
Backing Up and Restoring Mobility Services Engine Data	228
Backing Up Mobility Services Engine Historical Data	229
Restoring Mobility Services Engine Historical Data	229
Enabling Automatic Location Data Backup	230
Downloading Software to the Mobility Services Engines	230
Manually Downloading Software	231
Configuring the NTP Server	232
Resetting the System	232
Clearing the Configuration File	232

APPENDIX A

MSE System and Appliance Hardening Guidelines	233
--	------------

Setup Wizard Update	233
Configuring Future Restart Day and Time	233
Configuring the Remote Syslog Server to Publish MSE Logs	234
Configuring the Host Access Control Settings	234
Certificate Management	235
Creating a CSR	235
Importing the CA Certificate	236
Importing Server Certificate	236
Enabling or Disabling Client Certificate Validation	237
Configuring Online Certificate Status Protocol (OCSP) Settings	237
Importing a CRL	238
Clearing Certificate Configuration	238
Showing Certificate Configuration	239
Updated Open Port List	242
Syslog Support	242
MSE and RHEL 5	242



Preface

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

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

Audience

This guide is for administrators who configure and manage Context-Aware Service (CAS). Before you begin, you should be familiar with network structure, terms, and concepts.

Related Documentation

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

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

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

Obtaining Documentation and Submitting a Service Request

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

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



Overview

This chapter describes the role of the Cisco 3300 series Mobility Services Engine (MSE), a component of the Cisco Connected Mobile Experience, 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 CMX, is addressed.

- [About the Cisco Context-Aware Mobility Solution, page 1](#)
- [Licensing Information for Clients and Tags, page 3](#)
- [Viewing Contextual Information, page 3](#)
- [Event Notification, page 4](#)

About the Cisco Context-Aware Mobility Solution

The foundation of the CMX 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.

- [Cisco 3300 Series Mobility Services Engine, on page 1](#)
- [Context-Aware Service \(CAS\), on page 2](#)
- [ContextAware Tab, on page 2](#)

Cisco 3300 Series Mobility Services Engine

The Cisco 3300 series MSE operates with CAS, which is a component of the CMX solution.

There are two models of the MSE :

- Cisco 3355 Mobility Services Engine
- Virtual Appliance

Context-Aware Service (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 *Cisco Context-Aware Engine for Clients and Tags* for processing the contextual information it receives. The *Cisco Context-Aware Engine for Clients and Tags* processes data received from Wi-Fi clients and Wi-Fi tags.

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 five 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 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 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.

For more information about Location assisted client troubleshooting, see the [Location Assisted Client Troubleshooting from the ContextAware Dashboard](#), on page 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 the 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.

Licensing Information for Clients and Tags

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

- It is a common license for tags and clients (Base Location License).
- For more information on tags, clients, rogue clients, and rogue access points, see [Context-Aware Service Planning and Verification, on page 81](#).
- License for tags and clients are offered in various quantities, ranging from multiples of 1,10, and100 access points. Up to 50,000 Wi-Fi clients and Wi-Fi tags (combined count) are supported depending on the mobility services engine hardware.
- MSE 3355 can track up to 2500 APs and VM can track up to 5000 APs for Base and advanced location services. Maximum number of clients that can be tracked for MSE 3355 and VM are 25,000 and 50,000 respectively.

Viewing Contextual Information

The collected contextual information can be viewed in graphical user interface format in 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 3355 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 (WLC) 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.

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

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](#), on page 2.

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)
- Simple Network Management Protocol (SNMP)
- Syslog

**Note**

Prime Infrastructure can act as a listener receiving event notifications over SNMP. Without event notification, 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.



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 (MSE) to and from the Cisco Prime Infrastructure.



Note

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

- [Licensing Requirements for MSE, page 7](#)
- [Guidelines and Limitations, page 9](#)
- [Adding a Mobility Services Engine to the Prime Infrastructure, page 9](#)
- [Deleting an MSE License File, page 14](#)
- [Deleting a Mobility Services Engine from the Prime Infrastructure, page 14](#)
- [Registering Device and wIPS Product Authorization Keys, page 14](#)
- [Installing Device and wIPS License Files, page 15](#)

Licensing Requirements for MSE

See [Cisco Mobility Services Ordering and Licensing Guide](#) for MSE license information.

- [MSE License Structure Matrix, on page 8](#)
- [Sample MSE License File, on page 8](#)
- [Revoking and Reusing an MSE License, on page 9](#)

MSE License Structure Matrix

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

Table 1: MSE License Structure Matrix

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



Note

Contact Cisco account representative to extend evaluation licenses if required.

Sample MSE License File

The following is a sample MSE license file:

```
Feature MSE Cisco 1.0 permanent uncounted \
VENDOR_STRING=UDI=udi,COUNT=1 \
HOSTID=ANY \
NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</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 five license entries. First word in the first line of any license entry will tell you what type of license it is. It can either be a Feature or Increment license. A Feature license is static, lone-item license. An Increment license is an additive license. In the MSE, each service engine is treated as Increment licenses.

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

Revoking and Reusing an MSE License

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

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

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

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

Guidelines and Limitations

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

- From release 7.5 onwards, wIPS service requires a separate MSE.
- After adding a new MSE, you can synchronize network designs (campus, building, and outdoor maps), Cisco WLC, switches (Catalyst 3000 series and 4000 series only), and event groups for the Mobility Services Engine and the Prime Infrastructure.

**Note**

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

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

Adding a Mobility Services Engine to the Prime Infrastructure

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

**Tip**

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

**Note**

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

**Note**

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

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

-
- Step 1** Verify that you can ping the Mobility Services Engine.
- Step 2** Choose **Services > Mobility Services Engines** to display the Mobility Services page.
- Step 3** From the Select a command drop-down list, choose **Add Mobility Services Engine**, and click **Go**.
- Step 4** In the **Device Name** text box, enter a name for the MSE.
- Step 5** In the **IP Address** text box, enter the IP address of the MSE.
- Step 6** (Optional) In the **Contact Name** text box, enter the name of the MSE administrator.
- Step 7** In the **User Name** and **Password** text boxes, enter the username and password for the MSE. This refers to the Prime Infrastructure communication username and password created during the setup process. If you have not specified the username and password during the setup process, use the defaults. The default username and password are both *admin*.
- Note** If you changed the username and password during the automatic installation script, enter those values here. If you did not change the default passwords, we recommend that you rerun the automatic installation script and change the username and password.
- Step 8** Select the **HTTPS** check box to allow communication between the MSE and third-party applications. By default, the Prime Infrastructure uses HTTPSs to communicate with the MSE.
- Step 9** Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the MSE. This option is applicable for network designs, wired switches, Cisco WLCs, and event definitions. The existing location history data is retained, however, you must use manual service assignments to perform any future location calculations.
- Step 10** Click **Next**. The Prime Infrastructure automatically synchronizes the selected elements with the MSE. After the synchronization, the MSE License Summary page appears. You can use the MSE License Summary page to install a license, add a license, remove a license, install an activation license, and install service license. The Select Mobility Service page appears.
- Step 11** To enable a service on the Mobility Services Engine, select the check box next to the service. Services include Context-Aware Service and wIPS. You can choose CAS to track clients, rogues, interferers, wired clients, and tags. Choose Cisco Tag Engine to track tags.

Step 12 Click **Save**.

Note After adding a new MSE, you can synchronize network designs (campus, building, and outdoor maps), Cisco WLCs, switches (Catalyst Series 3000 only), and event groups on the local MSE using the Prime Infrastructure. You can perform this synchronization immediately after adding a new MSE or at a later time. To synchronize the local and the Prime Infrastructure databases, see [Synchronizing Mobility Services Engines](#), on page 17.

Enabling Services on the Mobility Services Engine

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

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

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

- Context Aware Service—If you select the Context Aware Service check box, then you must select a location engine to perform location calculation. You can choose **CAS to track clients, rogues, interferers, and tags**. You can choose Cisco Context-Aware Engine for Clients and Tag to track tags.
- Wireless Intrusion Prevention System—If you select the Wireless Intrusion Prevention System check box, it detects wireless and performance threats.
- Mobile Concierge Service—If you select the Mobile Concierge Service check box, it provides service advertisements that describe the available services for the mobile devices.
- CMX Analytics Service—If you select the CMX Analytics Service check box, it provides a set of data analytic tools packaged for analyzing Wi-Fi device location data that comes from the MSE.

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

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

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

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

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

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

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

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

Note If the history tracking is not enabled, the MSE service will not function.

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

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

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

- Map Name
- Type (building, floor, campus)
- Status

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

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

Configuring MSE Tracking and History Parameters

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

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

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

- Wired Clients
- Wireless Clients
- Rogue Access Points
 - Exclude Adhoc Rogue APs

- Rogue Clients
- Interferers
- Active RFID Tags

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

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

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

Assigning Maps to the MSE



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

To assign maps to the MSE, follow these steps:

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

- Map Name
- Type (building, floor, campus)
- Status

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

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

Deleting an MSE License File

To delete an MSE license file, follow these steps:

-
- Step 1** Choose **Services > Mobility Service Engine**.
The Mobility Services page appears.
 - Step 2** Click **Device Name** to delete a license file for a particular service. Select the Mobility Services Engine(s) to be deleted by selecting the corresponding **Device Name** check box(es).
 - Step 3** From the Select a command drop-down list, choose **Edit Configuration**.
The Edit Mobility Services Engine dialog box appears.
 - Step 4** Click **Next** in the Edit Mobility Services Engine dialog box.
The MSE License Summary page appears.
 - Step 5** Choose the MSE license file that you want to delete in the MSE License Summary page.
 - Step 6** Click **Remove License**.
 - Step 7** Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the license.
 - 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:

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

Registering Device and wIPS Product Authorization Keys

You receive a Product Authorization Key (PAK) when you order a CAS element, wIPS, or tag license from Cisco. You must register the PAK to receive the license file for installation on the Mobility Services Engine.

License files are e-mailed to you after successfully registering a PAK. Client and wIPS PAKs are registered with Cisco.

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

-
- Step 1** On your web browser, go to <http://tools.cisco.com/SWIFT/LicensingUI/Home>.
- Step 2** Enter the PAK, and click **SUBMIT**.
- Step 3** Verify the license purchase. Click **Continue** if correct. The licensee entry page appears.
Note If the license is incorrect, click the **TAC Service Request Tool** URL to report the problem.
- Step 4** In the Designate Licensee page, enter the UDI of the MSE in the Host Id text box. This is the Mobility Services Engine on which the license is installed.
Note UDI information for a Mobility Services Engine is found in the General Properties at **Services > Mobility Services Engine > Device Name > System**.
- Step 5** Select the **Agreement** check box. Registrant information appears beneath the Agreement check box.
- Step 6** If the registrant and end user are not the same person, select the **Licensee (End-User)** check box beneath registrant information and enter the information for the end user.
- Step 7** Click **Continue**. A summary of entered data appears.
- Step 8** In the Finish and Submit page, review registrant and end-user data. Click **Edit Details** to correct any information. Click **Submit**. A confirmation page appears.
-

Installing Device and wIPS License Files

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

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

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

-
- Step 1** Choose **Administration > License CenterLicenses**.
- Step 2** Choose **Files > MSE Files** from the left sidebar menu.
- Step 3** Click **Add**. The Add a License File dialog box appears.
- Step 4** Choose the applicable MSE name from the **MSE Name** drop-down list.
Note Verify that the UDI of the selected Mobility Services Engine matches the one that you entered when registering the PAK.

Step 5 Click **Choose FileBrowse** to select the license file.

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



Synchronizing Mobility Services Engines

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

**Note**

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

- [Synchronizing the Prime Infrastructure and Mobility Services Engines](#), page 17
- [Prerequisites for Synchronizing Mobility Services Engine](#), page 18
- [Working with Third-Party Elements](#), page 18
- [Synchronizing Cisco WLC with a Mobility Services Engine](#), page 19
- [Configuring Automatic Database Synchronization and Out-of-Sync Alerts](#), page 21
- [Viewing the Status of Mobility Services Engine Synchronization](#), page 23

Synchronizing the Prime Infrastructure and Mobility Services Engines

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

**Note**

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

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

- Network Design—A logical mapping of the physical placement of access points throughout facilities. A hierarchy of a single campus, the buildings that comprise that campus, and the floors of each building constitute a single network design.
- Cisco WLC—A selected Cisco WLC that is associated and regularly exchanges location information with a MSE. Regular synchronization ensures location accuracy.
- Wired Switches—Wired Catalyst switches that provide an interface to wired clients on the network. Regular synchronization ensures that location tracking of wired clients in the network is accurate.
 - The MSE can be synchronized with Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports.
 - The MSE can also be synchronized with the following Catalyst 4000 series switches: WS-C4948, WS-C4948-10GE, ME-4924-10GE, WS-4928-10GE, WS-C4900M, WS-X4515, WS-X4516, WS-X4013+, WS-X4013+TS, WS-X4516-10GE, WS-X4013+10GE, WS-X45-SUP6-E, and WS-X45-SUP6-LE.
- Event Groups—A group of predefined events that define triggers that generate an event. Regular synchronization ensures that the latest defined events are tracked. Event groups can also be created by third-party applications. For more information on third-party application created event groups, see the [Configuring Automatic Database Synchronization and Out-of-Sync Alerts, on page 21](#).
- Third Party Elements—When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.
- Service Advertisements—Mobile Concierge Service provides service advertisements on mobile devices. This shows the service advertisement that is synchronized with the MSE.

Prerequisites for Synchronizing Mobility Services Engine

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

Working with Third-Party Elements

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

Deleting the Elements or Marking Them as Third-Party Elements

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

-
- Step 1** Choose **Services > Synchronize Services**.
The Network Designs page appears.
- Step 2** In the Network Designs page, choose **Third Party Elements** from the left sidebar menu.
The Third Party Elements page appears.
- Step 3** Select one or more elements.
- Step 4** Click one of the following buttons:
- **Delete Event Groups**—Deletes the selected event groups.
 - **Mark as 3rd Party Event Group(s)**—Marks the selected event groups as third-party event groups.
-

Synchronizing Cisco WLC with a Mobility Services Engine

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

- [Assigning and Synchronizing Network Designs, a Cisco WLC, Catalyst Switch, or Event Group](#), on page 19
- [Assigning an MSE to the Cisco WLC](#), on page 20
- [Unassigning a Network Design, Wired Switch, or Event Group from MSE](#), on page 21

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

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

-
- Step 1** Choose **Services > Synchronize Services**.
The left sidebar menu contains the following options: **Network Designs**, **Controllers**, **Event Groups**, **Wired Switches**, **Third Party Elements**, and **Service Advertisements**.
- Step 2** From the left sidebar menu, choose the appropriate menu options.
- Step 3** To assign a network design to a MSE, in the Synchronize Services page, choose **Network Designs** from the left sidebar menu.

The Network Designs page appears.

- Step 4** Select all the maps to be synchronized with the MSE by selecting the corresponding **Name** check box.
- Note** Through Release 6.0, you can assign only up to a campus level to a MSE. Starting with Release 7.0, this option is granular to a floor level. For example, you can choose to assign floor1 to MSE 1, floor2 to MSE 2, and floor3 to MSE 3.
- Step 5** Click **Change MSE Assignment**.
- Step 6** Select the MSE to which the maps are to be synchronized.
- Step 7** Click either of the following in the MSE Assignment dialog box:

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

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

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

- Step 8** Click **Synchronize** to update the MSE(s) database(s).
When items are synchronized, a green two-arrow icon appears in the Sync. Status column for each synchronized entry. You can use the same procedure to assign wired switches or event groups to a MSE. To assign a Cisco WLC to a MSE, see the [Synchronizing Cisco WLC with a Mobility Services Engine](#) for more information.

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

Assigning an MSE to the Cisco WLC

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

- Step 1** Choose **Services > Synchronize Services**.
- Step 2** In the Network Designs page, choose **Controller** from the left sidebar menu.
- Step 3** Select the Cisco WLCs to be assigned to the Mobility Services Engine by selecting the corresponding **Name** check box.
- Step 4** Click **Change MSE Assignment**.
- Step 5** Choose MSEs dialogue box appears. You can choose **CAS**, **wIPS** or **MSAP** option.
- Step 6** Choose the MSE to which the Cisco WLCs must be synchronized.
- Step 7** Click either one of the following in the Choose MSEs dialog box:
- **Synchronize**—Synchronizes the MSE assignment.
 - **Cancel**—Discards the changes to MSE assignment and returns to the **Controllers** page.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configuring Automatic Database Synchronization and Out-of-Sync Alerts

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

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

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

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

- [Configuring Automatic Database Synchronization](#), on page 22
- [Smart Controller Assignment and Selection Scenarios](#), on page 22
- [Out-of-Sync Alarms](#), on page 23

Configuring Automatic Database Synchronization

To configure smart synchronization, follow these steps:

-
- Step 1** Choose **Administration > Background Tasks**.
- Step 2** Select the **Mobility Service Synchronization** check box and click the **Mobility Service Synchronization** link. The Mobility Services Synchronization page appears.
- Step 3** To set the Mobility Services Engine to send out-of-sync alerts, select the Out of Sync Alerts **Enabled** check box.
- Step 4** To enable smart synchronization, select the Smart Synchronization **Enabled** check box.
- Note** Smart synchronization does not apply to elements (network designs, controllers, or event groups) that have not yet been assigned to a MSE. However, out-of-sync alarms are still generated for these unassigned elements. For smart synchronization to apply to these elements, you must manually assign them to a MSE.
- Note** When a MSE is added to a Prime Infrastructure, the data in the Prime Infrastructure is always treated as the primary copy that is synchronized with the MSE. All synchronized network designs, controllers, event groups, and wired switches that are present in the MSE and not in the Prime Infrastructure are removed automatically from MSE.
- Step 5** Enter the time interval, in minutes, that the smart synchronization is to be performed. By default, the smart-sync is enabled.
- Step 6** Click **SubmitSave**.
For Smart controller assignment and selection scenarios, see the [Smart Controller Assignment and Selection Scenarios](#), on page 22.
-

Smart Controller Assignment and Selection Scenarios

Scenario 1

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

Scenario 2

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

Scenario 3

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

Scenario 4

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

Out-of-Sync Alarms

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

- Elements are modified in the Prime Infrastructure (the auto-sync policy pushes these elements).
- Elements other than Cisco WLCs exist in the Mobility Services Engine database but not in the Prime Infrastructure.
- Elements are not assigned to any MSE (the auto-sync policy does not apply).

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

- The MSE is deleted



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

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

Viewing the Status of Mobility Services Engine Synchronization

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

- [Viewing the Status of Mobility Services Engine Synchronization](#), on page 24
- [Viewing Synchronization History](#), on page 24

Viewing the Status of Mobility Services Engine Synchronization

To view the synchronization status, follow these steps:

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

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

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

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

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

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

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

Viewing Synchronization History

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

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

Table 2: Synchronization History Page

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

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



Configuring High Availability

This chapter describes how to configure high availability on the Cisco Mobility Services Engine. The MSE 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 to the secondary MSE.



Note

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

- [Overview of the High Availability Architecture, page 27](#)
- [Pairing Matrix, page 28](#)
- [Guidelines and Limitations for High Availability, page 28](#)
- [Failover Scenario for High Availability, page 29](#)
- [Failback Scenario for High Availability, page 29](#)
- [HA Licensing, page 29](#)
- [Configuring High Availability on the MSE, page 29](#)
- [Viewing Configured Parameters for High Availability, page 43](#)
- [Viewing High Availability Status, page 43](#)

Overview of 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.
- One secondary MSE can support one primary MSE.

Pairing Matrix

The following table lists the server type pairing matrix information.

Table 3: Pairing Matrix

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

Guidelines and Limitations for High Availability

- Both the health monitor IP and virtual IP should be accessible from Prime Infrastructure.
- The health monitor IP and virtual IP should always be different. The health monitor and virtual interface can be on the same network 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 should be reinitiated. The longer it takes to restore the failed MSE, the longer you are running with a single MSE without high availability 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 MSEs 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 occur:

- 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 starts immediately. If automatic failover is disabled, an e-mail is sent to the administrator asking if they want to manually start failover.
- When manual failover is configured, an e-mail is sent only if the e-mail is configured for MSE alarms.
- The result of the failover operation is indicated as an event in the Health Monitor UI, and a critical alarm is sent to Prime Infrastructure.

Failback Scenario for High Availability

When the primary MSE is restored to its normal state, if the secondary MSE is already in failover state 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.
- 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.
- Failback can occur only if the administrator starts up the failed primary MSE.

HA Licensing

For high availability, an activation license is required on the primary and secondary virtual appliances. No other service license is required on the secondary MSE. It is required only on the primary MSE.

Configuring High Availability on the MSE

During the installation of the MSE software (or using the MSE setup script), configure some critical elements. Pair up the primary and secondary MSE from the Prime Infrastructure UI.

**Note**

By default, all MSEs are configured as primary. If you do not want high availability support and are upgrading from an earlier release, you can continue to use the 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.

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

- Step 1** Ensure that the network connectivity between the primary and secondary MSEs 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 version is installed on the secondary MSE.
- Step 4** On the intended primary MSE, enter the following command:

```

/opt/mse/setup/setup.sh
-----
Welcome to the Cisco Mobility Services Engine Appliance Setup.

You may exit the setup at any time by typing <Ctrl+c>.
-----

Would you like to configre MSE using:
    1. Menu mode
    2. Wizard mode
Choose 1 or 2: 1
-----

Mobility Services Engine Setup

Please select a configuration option belwo and enter the
requested information. You may exit setup 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.

Please note that the following parameters are mandatory and must be configured at lease once.
-> Hostname
-> Network interface eth0
-> Timezone settings
-> Root password
-> NTP settings
-> Prime Infrastructure password

You must select option 24 to verify and apply any changes made during this session.
-----

PRESS <ENTER> TO CONTINUE:

-----

Configure MSE:

1) Hostname *                13) Remote syslog settings
2) Network interface eth0 settings*  14) Host access control settings
3) Timezone settings*        15) Audit Rules

```

- | | |
|-------------------------------------|--------------------------------------|
| 4) Root password * | 16) Login banner |
| 5) NTP settings * | 17) System console restrictions |
| 6) Prime Infrastructure password * | 18) SSH root access |
| 7) Display current configuration | 19) Single user password check |
| 8) Domain | 20) Login and password settings |
| 9) High availability role | 21) GRUB password |
| 10) Network interface eth1 settings | 22) Root access control |
| 11) DNS settings | 23) Auto start MSE on system boot up |
| 12) Future restart time | 24) ## Verify and apply changes ## |

Please enter your choice [1 - 24]:

Step 5 Configure the hostname:

Please enter your choice [1 - 24]: 1

Current Hostname=[mse]

Configure Hostname? (Y)es/(S)kip/(U)se default [Skip]: y

The host name 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.

Enter a Host name [mse]:mse1

Step 6 Configure the domain:

Please enter your choice [1-24]: 8

Current domain=[]

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

Step 7 Configure the Network interface eth0 settings.

Please enter your choice [1 - 24]: 2

Current eth0 interface IP address=[10.0.0.1]

Current eth0 interface netmask=[255.0.0.0]

Current IPv4 gateway address=[172.20.104.123]

Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:y

Enter an IP address for first ethernet interface of this machine.

Enter eth0 IP address [10.0.0.2]:

Enter the network mask for IP address 172.21.105.126

Enter network mask [255.255.255.224]:

Enter the default gateway address for this machine.

Note that the default gateway must be reachable from the first ethernet interface.

Enter default gateway address [172.20.104.123]:

Step 8 Configure the Root password:

Please enter your choice [1 - 24]: 4

Root password has not been configured
 Configure root password? (Y)es/(S)kip/(U)se default [Skip]:
 Changing password for user root.

You can now choose the new password.

A valid password should be a mix of upper and lower case letters, digits, and other characters. You can use an 8 character long password with characters from all of these classes. An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used.

Enter new password:

Step 9 Configure the High availability 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.

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

Enter a Virtual IP address for the Primary MSE server

Enter Virtual IP address [1.1.1.1]: 10.10.10.11

Enter network mask for IP address 10.10.10.1

Enter network mask [1.1.1.1]: 255.255.255.0

Select to start the sever in recovery mode.

You should choose yes only if this primary MSE was paired earlier and you have nowlost the

configuration from this box.

And, now you want to restore the configuration from Secondary via Cisco Prime Infrastructure
Do you wish to start this MSE in HA recovery mode?: (yes/no) [no]:**no**

Current IP address = [1.1.1.10]

Current eth0 netmask=[255.255.255.0]

Current gateway address=[1.1.1.1]

Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:

Enter an IP address for first ethernet interface of this machine.

Enter eth0 IP address [1.1.1.10]: 10.10.10.12

Enter the network mask for IP address 10.10.10.12

Enter network mask [255.255.255.0]:

Enter an default gateway address for this machine.

Note that the default gateway must be reachable from the first ethernet interface.

Enter default gateway address [1.1.1.1]:10.10.10.1

The second ethernet interface is currently disabled for this machine.

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

Step 10 Configure the Timezone settings:

Please enter your choice [1 - 24]: 3

Current Timezone=[America/New_York]

Configure Timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly.

Please select a continent or ocean.

- 1) Africa
- 2) Americas
- 3) Antarctica
- 4) Arctic Ocean
- 5) Asia
- 6) Atlantic Ocean
- 7) Australia
- 8) Europe
- 9) Indian Ocean
- 10) Pacific Ocean
- 11) UTC - I want to use Coordinated Universal Time.

#? 2

Please select a country.

- | | |
|----------------------|----------------|
| 1) Anguilla | 27) Honduras |
| 2) Antigua & Barbuda | 28) Jamaica |
| 3) Argentina | 29) Martinique |

- | | |
|------------------------|-----------------------------|
| 4) Aruba | 30) Mexico |
| 5) Bahamas | 31) Montserrat |
| 6) Barbados | 32) Netherlands Antilles |
| 7) Belize | 33) Nicaragua |
| 8) Bolivia | 34) Panama |
| 9) Brazil | 35) Paraguay |
| 10) Canada | 36) Peru |
| 11) Cayman Islands | 37) Puerto Rico |
| 12) Chile | 38) St Barthelemy |
| 13) Colombia | 39) St Kitts & Nevis |
| 14) Costa Rica | 40) St Lucia |
| 15) Cuba | 41) St Martin (French part) |
| 16) Dominica | 42) St Pierre & Miquelon |
| 17) Dominican Republic | 43) St Vincent |
| 18) Ecuador | 44) Suriname |
| 19) El Salvador | 45) Trinidad & Tobago |
| 20) French Guiana | 46) Turks & Caicos Is |
| 21) Greenland | 47) United States |
| 22) Grenada | 48) Uruguay |
| 23) Guadeloupe | 49) Venezuela |
| 24) Guatemala | 50) Virgin Islands (UK) |
| 25) Guyana | 51) Virgin Islands (US) |
| 26) Haiti | |

#? 47

Please select one of the following time zone regions.

- 1) Eastern Time
- 2) Eastern Time - Michigan - most locations
- 3) Eastern Time - Kentucky - Louisville area
- 4) Eastern Time - Kentucky - Wayne County
- 5) Eastern Time - Indiana - most locations
- 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
- 7) Eastern Time - Indiana - Pulaski County
- 8) Eastern Time - Indiana - Crawford County
- 9) Eastern Time - Indiana - Pike County
- 10) Eastern Time - Indiana - Switzerland County
- 11) Central Time
- 12) Central Time - Indiana - Perry County
- 13) Central Time - Indiana - Starke County
- 14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
- 15) Central Time - North Dakota - Oliver County
- 16) Central Time - North Dakota - Morton County (except Mandan area)
- 17) Mountain Time
- 18) Mountain Time - south Idaho & east Oregon
- 19) Mountain Time - Navajo
- 20) Mountain Standard Time - Arizona
- 21) Pacific Time
- 22) Alaska Time
- 23) Alaska Time - Alaska panhandle
- 24) Alaska Time - Alaska panhandle neck
- 25) Alaska Time - west Alaska
- 26) Aleutian Islands
- 27) Hawaii

#? 21

The following information has been given:

```
United States
Pacific Time
```

```
Therefore TZ='America/Los_Angeles' will be used.
Local time is now:      Sun Apr  6 18:45:27 PDT 2014.
Universal Time is now:  Mon Apr  7 01:45:27 UTC 2014.
Is the above information OK?
1) Yes
2) No
#? 1
```

Step 11 Configure the DNS settings:

```
Please enter your choice [1 - 24]: 11
```

```
Domain Name Service (DNS) Setup
```

```
Enable DNS (yes/no) [no]: y
Default DNS server 1=[8.8.8.8]
Enter primary DNS server IP address:
DNS server address must be in the form #.#.#.#, where # is 0 to 255 or hexadecimal :
separated v6 address
```

```
Enter primary DNS server IP address [8.8.8.8]:
Enter backup DNS server IP address (or none) [none]:
```

Step 12 Configure the NTP settings:

```
Please enter your choice [1 - 24]: 5
```

```
Network Time Protocol (NTP) Setup.
```

```
If you choose to enable NTP, the system time will be
configured from NTP servers that you select. Otherwise,
you will be prompted to enter the current date and time.
```

```
NTP is currently disabled.
Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y
```

```
Enter whether or not you would like to set up the
Network Time Protocol (NTP) for this machine.
```

```
If you choose to enable NTP, the system time will be
configured from NTP servers that you select. Otherwise,
you will be prompted to enter the current date and time.
```

```
Enable NTP (yes/no) [no]: y
Default NTP server 1=[time.nist.gov]
Enter NTP server name or address:
NTP server address must be in the form #.#.#.3, where # is 0 to 255 hexadecimal :
separated v6 address.
```

```

Enter NTP server name or [time.nist.gov]:
Enter another NTP server IP address (or none) [none]:
Configure NTP Authentication ? (Y)es/(S)kip/(U)se default [Skip]: y
Enter NTP Auth key Number [1]:
Enter NTP Auth key Value (String) [Secret]:
Do you want to continue (yes/no) [no]: y

```

Step 13 Configure the Prime Infrastructure password:

```
Please enter your choice [1 - 24]: 6
```

```

Cisco Prime Infrastructure communication password has not been configured.
Configure Prime Infrastructure password? (Y)es/(S)kip/(U)se default [Yes]:

```

```

Enter a password for the admin user.
The admin user is used by the Prime Infrastructure and other northbound systems to authenticate
their SOAP/XML session with the server. Once this password is updated, it must correspondingly
be updated on the NCS page for MSE General Parameters so that the Prime Infrastructure can
communicate with the MSE.

```

Step 14 Verify and apply changes

```
Please enter your choice: 24
```

```
Please verify the following setup information.
```

```

-----BEGIN-----

Hostname=mse1
Role= 1, Health Monitor Intercace=eth0, Direct connect interface=none
Virtual IP Address=10.10.10.11, Virtual IP Netmask=255.255.255.0
Eth0 IP address=10.10.10.12, Eth0 network mask=255.0.0.0
Default Gateway=10.10.10.1
Time zone=America/Los_Angeles
Enable DNS=yes, DNS servers=8.8.8.8
Enable NTP=yes, NTP servers=time.nist.gov
Time zone=America/Los_Angeles
Root password is changed.
Cisco Prime Infrastructure password is changed.

-----END-----

```

```
You may enter "yes" to proceed with configuration, "no" to make
more changes.
```

```

Configuration Changed
Is the above information correct (yes or no): yes

```

```
-----
Checking mandatory configuration information...
```

```
Root password: Not configured
```

```
**WARNING**
The above parameters are mandatory and need to be configured.
```

```
-----
Ignore and proceed (yes/no): yes
Setup will now attempt to apply the configuration.
Restarting network services with new settings.
Shutting down interface eth0:
```

The system is minimally configured right now. It is strongly recommended that you run the setup script under /opt/mse/setup/setup.sh command to configure all appliance related parameters immediately after installation is complete.

PRESS <ENTER> TO EXIT THE INSTALLER:

Step 15

Reboot the system:

```
[root@mse1]# reboot
Stopping MSE Platform
```

```
Flushing firewall rules:                [OK]
Setting chains to policy ACCEPT: nat filter          [OK]
Unloading iptables modules:                [ok]
```

Broadcast message from root (pts/0) (Tue Apr29 14:15:27:2014):

The system is going down for reboot NOW:

Step 16

Start the MSE services:

```
[root@mse1]# /etc/init.d/mseed start
Starting MSE Platform.
```

```
Starting Health Monitor, Waiting to check the status.
Starting Health Monitor, Waiting to check the status.
Health Monitor successfully started
Starting Admin process...
Started Admin process.
Starting database .....
Database started successfully. Starting framework and services.....
Framework and services successfully started
```

Step 17

After all services have started, confirm MSE services are working properly by entering the following command:

```
[root@mse1]# getserverinfo
```

Step 18

After the new installation, the initial login starts the Setup wizard where in you can configure the secondary MSE.

```
Current hostname=[mse1]
Configure hostname? (Y)es/(S)kip/(U)se default [Yes]: yes
```

The host name 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.

```
Enter a hostname [mse]: mse2
```

Step 19 Configure the domain:

```
Please enter your choice [1-24]: 8
Current domain=[ ]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: S
```

Step 20 Configure the High availability 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
```

```
-----
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.
```

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

```
Current IP address=[1.1.1.10]
Current eth0 netmask=[255.255.255.0]
Current gateway address=[1.1.1.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Yes]:
```

```
Enter an IP address for first ethernet interface of this machine.
```

```
Enter eth0 IP address [1.1.1.10]: 10.10.10.13
```

```
Enter the network mask for IP address 10.10.10.13
```

```
Enter network mask [255.255.255.0]:
```

```
Enter an default gateway address for this machine.
```

```
Note that the default gateway must be reachable from the first ethernet interface.
```

```
Enter default gateway address [1.1.1.1]:10.10.10.1
```

```
The second ethernet interface is currently disabled for this machine.
```

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

Step 21 Configure the Timezone settings:

Please enter your choice [1 - 24]: 3

Current Timezone=[America/New_York]

Configure Timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly.

Please select a continent or ocean.

- 1) Africa
- 2) Americas
- 3) Antarctica
- 4) Arctic Ocean
- 5) Asia
- 6) Atlantic Ocean
- 7) Australia
- 8) Europe
- 9) Indian Ocean
- 10) Pacific Ocean
- 11) UTC - I want to use Coordinated Universal Time.

#? 2

Please select a country.

- | | |
|------------------------|-----------------------------|
| 1) Anguilla | 27) Honduras |
| 2) Antigua & Barbuda | 28) Jamaica |
| 3) Argentina | 29) Martinique |
| 4) Aruba | 30) Mexico |
| 5) Bahamas | 31) Montserrat |
| 6) Barbados | 32) Netherlands Antilles |
| 7) Belize | 33) Nicaragua |
| 8) Bolivia | 34) Panama |
| 9) Brazil | 35) Paraguay |
| 10) Canada | 36) Peru |
| 11) Cayman Islands | 37) Puerto Rico |
| 12) Chile | 38) St Barthelemy |
| 13) Colombia | 39) St Kitts & Nevis |
| 14) Costa Rica | 40) St Lucia |
| 15) Cuba | 41) St Martin (French part) |
| 16) Dominica | 42) St Pierre & Miquelon |
| 17) Dominican Republic | 43) St Vincent |
| 18) Ecuador | 44) Suriname |
| 19) El Salvador | 45) Trinidad & Tobago |
| 20) French Guiana | 46) Turks & Caicos Is |
| 21) Greenland | 47) United States |
| 22) Grenada | 48) Uruguay |
| 23) Guadeloupe | 49) Venezuela |
| 24) Guatemala | 50) Virgin Islands (UK) |
| 25) Guyana | 51) Virgin Islands (US) |

#? 47

Please select one of the following time zone regions.

- 1) Eastern Time
- 2) Eastern Time - Michigan - most locations

- 3) Eastern Time - Kentucky - Louisville area
 - 4) Eastern Time - Kentucky - Wayne County
 - 5) Eastern Time - Indiana - most locations
 - 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 - 7) Eastern Time - Indiana - Pulaski County
 - 8) Eastern Time - Indiana - Crawford County
 - 9) Eastern Time - Indiana - Pike County
 - 10) Eastern Time - Indiana - Switzerland County
 - 11) Central Time
 - 12) Central Time - Indiana - Perry County
 - 13) Central Time - Indiana - Starke County
 - 14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
 - 15) Central Time - North Dakota - Oliver County
 - 16) Central Time - North Dakota - Morton County (except Mandan area)
 - 17) Mountain Time
 - 18) Mountain Time - south Idaho & east Oregon
 - 19) Mountain Time - Navajo
 - 20) Mountain Standard Time - Arizona
 - 21) Pacific Time
 - 22) Alaska Time
 - 23) Alaska Time - Alaska panhandle
 - 24) Alaska Time - Alaska panhandle neck
 - 25) Alaska Time - west Alaska
 - 26) Aleutian Islands
 - 27) Hawaii
- #? 21

The following information has been given:

```

United States
Pacific Time

```

```

Therefore TZ='America/Los_Angeles' will be used.
Local time is now:      Sun Apr  6 18:45:27 PDT 2014.
Universal Time is now: Mon Apr  7 01:45:27 UTC 2014.
Is the above information OK?
1) Yes
2) No
#? 1

```

Step 22 Configure the NTP settings:

Please enter your choice [1 - 24]: 5

Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

```

NTP is currently disabled.
Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

```

Enter whether or not you would like to set up the

Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

```
Enable NTP (yes/no) [no]: y
Default NTP server 1=[time.nist.gov]
Enter NTP server name or address:
NTP server address must be in the form #.#.#.3, where # is 0 to 255 hexadecimal :
separated v6 address.
Enter NTP server name or [time.nist.gov]:
Enter another NTP server IP address (or none) [none]:
Configure NTP Authentication ? (Y)es/(S)kip/(U)se default [Skip]: y
Enter NTP Auth key Number [1]:
Enter NTP Auth key Value (String) [Secret]:
Do you want to continue (yes/no) [no]: y
```

Step 23 Verify and apply changes

Please enter your choice: 24

Please verify the following setup information.

```
-----BEGIN-----

Hostname=mse2
Role= 2, Health Monitor Intercace=eth0, Direct connect interface=none
Eth0 IP address=10.10.10.13, Eth0 network mask=255.255.255.0
Default Gateway=10.10.10.1
Time zone=America/Los_Angeles
Enable NTP=yes, NTP servers=time.nist.gov
Time zone=America/Los_Angeles

-----END-----
```

You may enter "yes" to proceed with configuration, "no" to make more changes.

```
Configuration Changed
Is the above information correct (yes or no): yes
```

```
-----
Checking mandatory configuration information...
```

```
Root password: Not configured
```

```
**WARNING**
```

```
The above parameters are mandatory and need to be configured.
```

```
-----
Ignore and proceed (yes/no): yes
Setup will now attempt to apply the configuration.
```

```
Restarting network services with new settings.
Shutting down interface eth0:
```

```
The system is minimally configured right now. It is strongly recommended that you run the setup
script under /opt/mse/setup/setup.sh command to configure all appliance related parameters
immediately after installation is complete.
```

```
PRESS <ENTER> TO EXIT THE INSTALLER:
```

Step 24

Reboot the system:

```
[root@mse2 installers]# reboot
Stopping MSE Platform
```

```
Flushing firewall rules: [OK]
Setting chains to policy ACCEPT: nat filter [OK]
Unloading iptables modules: [ok]
```

```
Broadcast message from root (pts/0) (Tue Apr29 14:15:27:2014):
```

```
The system is going down for reboot NOW:
```

Step 25

Start the MSE services:

```
[root@mse2]# /etc/init.d/mseed start
Starting MSE Platform.
```

```
Starting Health Monitor, Waiting to check the status.
Starting Health Monitor, Waiting to check the status.
Health Monitor successfully started
Starting Admin process...
Started Admin process.
Starting database .....
Database started successfully. Starting framework and services.....
Framework and services successfully started
```

Step 26

Once you configure 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 27

Once you add the primary MSE successfully, choose **Services > High Availability** or click the primary MSE device in the **Services > Mobility Services Engine > System > Services High Availability > HA Configuration**. The HA Configuration page appears.

Step 28

Enter the secondary device name with which you want to pair the primary MSE.

Step 29

Enter the secondary IP address which is the health monitor IP address of the secondary MSE.

Step 30

Enter the secondary password. This is the Prime Infrastructure communication password configured on the MSE.

Step 31

Specify the failover type. You can choose either **Manual** or **Automatic** from the Failover Type drop-down list.

Step 32

Specify the failback type by choosing either **Manual** or **Automatic** from the Failback Type drop-down list.

Step 33

Specify the Long Failover Wait in seconds.
After 10 seconds, the system fails over. The maximum failover wait is two minutes.

Step 34

Click **Save**.
The pairing and the synchronization happens automatically.

- Step 35** To check whether the heartbeat is received from the primary MSE or not, choose **Services > Mobility Services Engine > System > Services High Availability > HA Status**.
-

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 **MSE 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 provides 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 **MSE Name** to view the desired status.
The HA Configuration page appears.
- Step 3** Choose **HA Status** from the left sidebar menu. The HA Configuration page provides 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.
-



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.

- [Physical Appliance, page 45](#)
- [Virtual Appliance, page 45](#)
- [Viewing the MSE License Information Using the License Center, page 46](#)
- [Removing a License File Using the License Center, page 47](#)

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 Unique Device Identifier (UDI). 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

The MSE is also offered as a virtual appliance, to support lower-level, high, and very high deployments. When the MSE is located on the virtual appliance, the license is validated against Virtual Unique Device Identifier (VUDI) 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 the **Administration > License Center** page to add or delete a license.

See the [Adding and Deleting Mobility Services Engines and Licenses](#) and the [Deleting an MSE License File, on page 14](#) for more information on adding a license and deleting a license using the mobility services engine wizard.

For more details on deploying MSE virtual appliance, see the *Cisco MSE Virtual Appliance Configuration Guide*.

This section contains the following topics:

- [Operating Systems Requirements](#)
- [Client Requirements](#)
- [Virtual Appliance Sizing](#)
- [Reinstalling MSE on a Physical Appliance](#)
- [Deploying the MSE Virtual Appliance](#)
- [Adding a License File to the MSE Using the License Center](#)

Viewing the MSE License Information Using the License Center

The license center allows you to manage the Prime Infrastructure, Cisco WLCs, 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. The following table lists the MSE Summary page fields.

Table 4: MSE Summary Page

Field	Description
MSE Name	Provides a link to the MSE license file list page.

Field	Description
Service	The service type can be CAS, wIPS, Mobile Concierge service, Location Analytics service, Billboard service, and Proxy service.
Platform Limit	Platform limit.
Type	Specifies the type of MSE.
Installed Limit	Shows the total number of client access points 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.

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 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.
-



Configuring and Viewing System Properties

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

- [Licensing Requirement, page 49](#)
- [Editing General Properties and Viewing Performance, page 49](#)
- [Modifying NMSP Parameters, page 52](#)
- [Viewing Active Sessions on a System, page 54](#)
- [Adding and Deleting Trap Destinations, page 54](#)
- [Viewing and Configuring Advanced Parameters, page 56](#)

Licensing Requirement

All Mobility Services Engines are shipped with an evaluation license of CAS and wIPS. Evaluation copies are good for a period of 60 days (480 hours) and have preset device limits for each service. They are provided with a 120 day license (time is decremented by the number of days you use it rather than by the number of calendar days passed).

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

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

Editing General Properties and Viewing Performance

General Properties—You can use the Cisco Prime Infrastructure to edit the general properties of a Mobility Services Engine such as contact name, username, password, services enabled on the system, enabling or disabling a service, or enabling the MSE for synchronization. See the [Editing General Properties, on page 50](#) for more information.



Note

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

Performance—You can use the Prime Infrastructure to view CPU and memory usage for a given MSE. See the [Viewing Performance Information, on page 52](#) for more information.

This section contains the following topics:

- [Editing General Properties, on page 50](#)
- [Viewing Performance Information, on page 52](#)

Editing General Properties

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

- Step 1** Choose **Services > Mobility Services > Mobility Services Engines** to display the Mobility Services page.
- Step 2** Click the name of the MSE you want to edit. Two tabs appear with the following headings: General and Performance.
Note If the General Properties page is not displayed by default, choose **Systems > General Properties** from the left sidebar menu.
- Step 3** Modify the fields as appropriate on the General tab. This table lists the General Properties page fields.

Table 5: General Tab

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

Field	Configuration Options
Legacy HTTPS	This does not apply to MSEs. 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 MSE. This option shows up only if the delete synchronized service assignments check box was unselected while adding a MSE.
Mobility Services	<p>To enable a service on the MSE, select the check box next to the service. The services include Context Aware, wIPS, Mobile Concierge, CMX Analytics, CMX Browser Engage, and Proxy service.</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 <p>or</p> <ul style="list-style-type: none"> • Partner Tag Engine <p>Note The Partner Tag Engine is used only to track the tags. The clients are still tracked by Cisco Context-Aware Engine.</p> <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 From release 7.5 onward, wIPS service requires a dedicated MSE because it does not support CAS and wIPS on the same MSE.</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 MSEs on the network.</p> <p>Note For more information on purchasing and installing licenses, see the following URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html</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: , tcp 8001: Legacy port. Used for location APIs.

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

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

Step 4

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

Viewing Performance Information

To view performance details, follow these steps:

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

Modifying NMSP Parameters

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

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

- We recommend no change in the default parameter values unless the network is expecting slow response or excessive latency.
- Telemetry, emergency, and chokepoint information is only seen on controllers and the Prime Infrastructure installed with software Release 4.1 and later.
- The TCP port (16113) that the controller and MSE communicate over must be open (not blocked) on any firewall that exists between the controller and MSE for NMSP to function.

To configure NMSP parameters, follow these steps:

-
- Step 1** Choose **Services > Mobility Services > Mobility Services Engines**.
- Step 2** Click the name of the MSE whose properties you want to edit.
- Step 3** Choose **System > NMSP Parameters**. The configuration options appear.
- Step 4** Modify the NMSP parameters as appropriate. The following table lists the NMSP parameters.

Table 6: NMSP Parameters

Field	Description
IP Address	IP address of the controller or IOS 3E switch.

Field	Description
Target Type	Type of the controller: Controller or IOS 3E switch.
Version	Version of the target device.
NMSP Status	NMSP connection status between MSE and target type.
Echo Request Count	Number of echo request made.
Echo Response Count	Number of echo requests received.
Last Message Received	Timestamp when the last message was received.

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

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

Viewing Active Sessions on a System

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

To view active user sessions, follow these steps:

-
- Step 1** Choose **Services > Mobility Services**.
- Step 2** Click the name of the MSE to view its active sessions.
- Step 3** Choose **System > Active Sessions**.
For every session, the Prime Infrastructure shows the following information:
- Session identifier
 - IP address from which the MSE is accessed
 - Username of the connected user
 - Date and time when the session started
 - Date and time when the MSE was last accessed
 - How long the session was idle since it was last accessed
-

Adding and Deleting Trap Destinations

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

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

- [Adding Trap Destinations, on page 55](#)
- [Deleting Trap Destinations, on page 56](#)

Adding Trap Destinations

To add a trap destination, follow these steps:

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

The following table lists the Add Trap Destination page fields.

Table 7: Add Trap Destination Page Fields

Field	Description
IP Address	IP address for the trap destination.
Port Number	The port number for the trap destination. The default port number is 162.
Destination Type	This field is not editable and has a value of Other .
SNMP Version	Choose either v2c or v3 from the SNMP Version drop-down list.
The following set of fields appear only if you select v3 as the SNMP version.	
User Name	The username for the SNMP Version 3.
Security Name	The security name for the SNMP Version 3.
Authentication Type	Choose one of the following from the drop-down list: HMAC-MD5 HMAC-SHA
Authentication Password	The authentication password for the SNMP Version 3.
Privacy Type	Choose one of the following from the drop-down list: CBC-DES CFB-AES-128 CFB-AES-192 CFB-AES-256
Privacy Password	The privacy password for the SNMP Version 3.

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

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

Deleting Trap Destinations

To delete a trap destination, follow these steps:

- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the Mobility Services Engine for which you want to delete a SNMP trap destination server.
- Step 3** Choose **System > Trap Destinations**.
- Step 4** Select the check box next to the trap destination entry that you want to delete.
- Step 5** From the Select a command drop-down list, choose **Add Trap Destination**. Click **Go**.
- Step 6** In the dialog box that appears, click **OK** to confirm deletion.
-

Viewing and Configuring Advanced Parameters

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

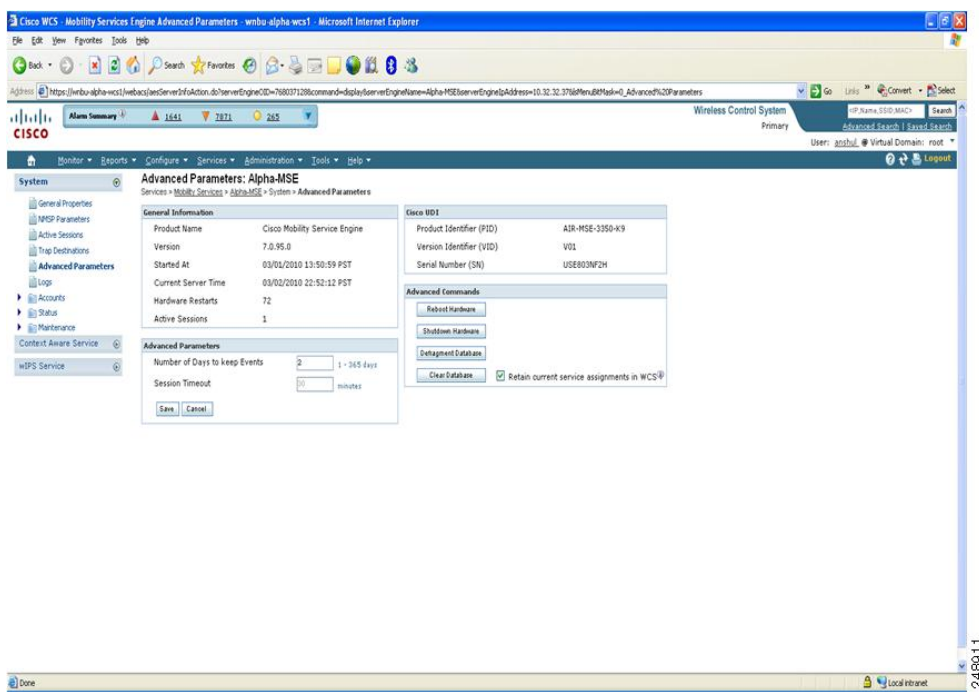
- See the [Viewing Advanced Parameter Settings](#) to view current system- level advanced parameters.
- See the [Initiating Advanced Commands](#) to modify the current system- level advanced parameters or initiate advanced commands such as system reboot, system shut down, or clear a configuration file.

Viewing Advanced Parameter Settings

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

- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of a Mobility Services Engine to view its status.
- Step 3** Choose **System > Advanced Parameters**. The Advanced Parameters page appears.

Figure 1: Advanced Parameters Page



Initiating Advanced Parameters

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



Note

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

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

- To set how long events are kept and how long before a session times out.
For more information, see the [Configuring Advanced Parameters](#).
- To initiate a system reboot or shutdown, or clear the system database.
For more information, see the [Initiating Advanced Commands](#).

Configuring Advanced Parameters

To configure advanced parameters, follow these steps:

-
- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of the mobility service whose properties you want to edit.
- Step 3** From the left sidebar menu, choose **System > Advanced Parameters**.
- Step 4** View or modify the advanced parameters as necessary.
- General Information
 - Product Name
 - Version
 - Started At
 - Current Server Time
 - Hardware Resets
 - Active Sessions
 - Advanced Parameters

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

 - Number of Days to keep Events—Enter the number of days to keep logs. Change this value as required for monitoring and troubleshooting.
 - Session Timeout—Enter the number of minutes before a session times out. Change this value as required for monitoring and troubleshooting. Currently this option appears dimmed.
 - Cisco UDI
 - Product Identifier (PID)—The product ID of the MSE.
 - Version Identifier (VID)—The version number of the MSE.
 - Serial Number (SN)—Serial number of the MSE.
 - Advanced Commands
 - Reboot Hardware—Click to reboot the mobility services hardware. See the [Rebooting or Shutting Down a System](#), on page 59 for more information.

- Shutdown Hardware—Click to turn off the mobility services hardware. See the [Rebooting or Shutting Down a System, on page 59](#) for more information.
- Clear Database—Click to clear the mobility services database. See the [Clearing the System Database, on page 59](#) for more information. Unselect the **Retain current service assignments in Prime Infrastructure** check box to remove all existing service assignments from the Prime Infrastructure and MSE. The resources must be reassigned in the **Services > Synchronize Services** page. By default, this option is selected.

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

Initiating Advanced Commands

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

- [Rebooting or Shutting Down a System](#)
- [Clearing the System Database](#)

Rebooting or Shutting Down a System

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

-
- Step 1** Choose **Services > Mobility Services Engines**.
- Step 2** Click the name of a Mobility Services Engine you want to reboot or shut down.
- Step 3** Choose **System > Advanced Parameters**.
- Step 4** In the Advanced Commands group box, click the appropriate button (**Reboot Hardware** or **Shutdown Hardware**). Click **OK** in the confirmation dialog box to initiate either the reboot or shutdown process. Click **Cancel** to stop the process.
-

Clearing the System Database

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

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

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

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

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



Mobile Concierge Services

Cisco Mobile Concierge service provides requirements for mobile clients and servers, and describes message exchanges between them. The Mobile Concierge solution delivers a unique in-store experience to customers who use smartphones.

Mobile Concierge service is used by the mobile devices that are configured with a set of policies for establishing network connectivity. Mobile Concierge service facilitates mobile devices to discover network-based services available in a local network or services that are enabled through service providers. Once you are connected to the stores Wi-Fi network, you receive different services including electronic coupons, promotional offers, customer loyalty data, product suggestions, and so on.

- [Licensing for Mobile Concierge, page 61](#)
- [Defining a Venue, page 62](#)
- [Deleting the Venue, page 63](#)
- [Adding New Service Providers with Policies, page 63](#)
- [Adding New Service Providers with Policies, page 64](#)
- [Deleting a Service Provider, page 65](#)
- [Defining New Policies, page 65](#)
- [Deleting Policies, page 66](#)

Licensing for Mobile Concierge

You can enable Mobile Concierge service only if you have a valid Advanced Location service license. If you have the Base Location license, you can upgrade to Advanced Location services by buying the Upgrade SKUs. For information on SKUs, see the *Release Notes for Cisco 3300 Series Mobility Services Engine, Release 7.5*.

Defining a Venue

To define a venue, follow these steps:

-
- Step 1** Choose **Services > Mobile Concierge**.
- Step 2** Choose **Mobile Concierge Services > Venues** from the left sidebar menu. The venue page appears.
- Step 3** From the Select a command drop-down list, choose **Define New Venue**, and click **Go**. The Venue Wizard page appears.
- Step 4** Enter the venue name in the Venue Name text box, and click **Next**.
- Step 5** In the Floor/Outdoor Association group box, do the following:
- 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**.
- Note** The Building, Floor Area, and Coverage Area drop-down lists are displayed only when you select Floor Area as the area type.
- From the Campus drop-down list, choose the campus name where you want to display the service advertisements.
 - From the Building drop-down list, choose the building name where you want the advertisements to appear.
 - From the Floor drop-down list, choose the floor type.
 - From the Coverage Area drop-down list, choose the coverage area within the floor.
 - From the Outdoor Area drop-down list, choose the outdoor area where you want to display the service advertisements. This field is displayed only if you select Outdoor Area as the Area Type.
- Step 6** Click **Next**. The Audio group box appears.
- Step 7** In the Audio group box, click **Choose File** to browse and select the audio file to play the audio notification on the mobile device.
- Step 8** Click **Next**. The Icons group box appears.
- Step 9** In the Icons group box, click **Choose File** to browse and select the icon.
- Step 10** Click **Next**. The Venue Apps group box appears.
- Step 11** In the Venue Apps group box, choose the venue where you want to broadcast the service advertisements.
- Step 12** Click **Next**. The Additional Venue Information group box appears.
- Step 13** In the Additional Information group box, do the following:
- Enter the location detail in the Location Detail text box. This provides location details such as store address, zip code, or street address of the venue.
 - Enter the GPS latitude and longitude of the venue in the Latitude and Longitude text box. This helps the applications to identify the venue accurately.
 - Enter any other additional information that you want to provide in the Additional Information text box.

Step 14 Click **Save**. This information is applied to the MSE and the synchronization happens automatically.

Deleting the Venue

To delete a venue, follow these steps:

-
- Step 1** Choose **Services > Mobile Concierge**.
The Venues page appears.
- Step 2** Select the check box of the venue that you want to delete.
- Step 3** From the Select a command drop-down list, choose **Delete Venue**, and click **Go**.
- Step 4** Click **OK** to confirm the deletion.
-

Adding New Service Providers with Policies

To add a service provider with policies, follow these steps:

-
- Step 1** Choose **Service > Mobile Concierge**.
- Step 2** Choose **Mobile Concierge Services > Providers** from the left sidebar menu.
The Providers page appears.
- Step 3** From the Select a command drop-down list, choose **Define New Provider**, and click **Go**.
The Provider Wizard page appears.
- Step 4** Enter the service providers venue name in the Provider Name text box.
- Step 5** Click **Next**. The Icons group box appears.
- Step 6** Select an icon that is associated with the service provider by clicking **Choose File**. This is the icon that is displayed on the clients handset.
- Step 7** Click **Next**. The Local Services group box appears.
- Step 8** In the Local Services group box, do the following:
- Click the blue inverted triangle icon located at the left side of the Local Service # name to expand the Local Service and configure the following:
 - Choose the service type from the Service Type drop-down list. The possible options are: **Directory Info**, **Sign Up**, **Discount Coupon**, **Network Help**, and **Other**.
 - Enter the name that you want to display on the clients handset in the Display Name text box.
 - Enter the service description in the Description text box.

- Choose the service URIs from the Service URI drop-down list.

Step 9 Click **Save**. This information is applied to the MSE and synchronization happens automatically.

Adding New Service Providers with Policies

To add a service provider with policies, follow these steps:

Step 1 Choose **Service > Mobile Concierge**.

Step 2 Choose **Mobile Concierge Services > Providers** from the left sidebar menu. The Providers page appears.

Step 3 From the Select a command drop-down list, choose **Define New Provider** and click **Go**. The Provider Wizard page appears.

Step 4 Enter the service providers venue name in the Provider Name text box.

Step 5 Click **Next**. The Icons group box appears.

Step 6 Select an icon that is associated with the service provider by clicking **Choose File**. This is the icon that is displayed on the clients handset.

Step 7 Click **Next**. The Local Services group box appears.

Step 8 In the Local Services group box, do the following:

- Click the blue inverted triangle icon location at the left side of the Local Service # name to expand the Local Service and configure the following:
 - Choose the service type from the Service Type drop-down list. The possible options are: **Directory Info**, **Sign Up**, **Discount Coupon**, **Network Help**, and **Other**.
 - Enter the name that you want to display on the clients handset in the Display Name text box.
 - Enter the service description in the Description text box.
 - Choose the service URIs from the Service URI drop-down list.

Step 9 Click **Save**. This information is applied to the MSE and synchronization happens automatically.

Deleting a Service Provider

To delete a service provider, follow these steps:

-
- Step 1** Choose **Services > Mobile Concierge**.
The Venue page appears.
 - Step 2** Choose **Mobile Concierge Services > Providers** from the left sidebar menu.
The Providers page appears.
 - Step 3** Select the check box of the service provider that you want to delete.
 - Step 4** From the Select a command drop-down list, choose **Delete Provider**, and click **Go**.
Click **OK** to confirm the deletion.
-

Defining New Policies

To define new policies, follow these steps:

-
- Step 1** Choose **Services > Mobile Concierge**.
 - Step 2** Choose **Mobile Concierge Services > Policies** from the left sidebar menu.
The Policies page appears.
 - Step 3** From the Select a command drop-down list, choose **Define New Policy**, and click **Go**.
The Policy Wizard page appears.
 - Step 4** Choose the venue on which you want the policy to be applied from the Venue drop-down list.
 - Step 5** Click **Next**. The Provider group box appears.
 - Step 6** Choose the service provider from the Provider drop-down list.
 - Step 7** Click **Next**.
 - Step 8** From the SSID drop-down list, choose the SSIDs on which you want to broadcast the service advertisements, and click **OK**. You can choose multiple SSIDs.
 - Step 9** Click **Next**. The Display Rule group box appears.
 - Step 10** In the Display Rule group box, do the following:
Select the Display Rule radio button. You can select either **Display Everywhere** or **Display Near selected APs** radio button. By default, Display everywhere is selected.

If you select Display everywhere, it searches for all the Mobile Concierge-supported Cisco WLCs that provide these SSIDs and assigns these controllers to the MSE.

If you select Display near selected APs, 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 broadcast. The service advertisement is displayed when the mobile device is near the radio band that you 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 11 Click **Finish**.

Deleting Policies

To delete a policy, follow these steps:

- Step 1** Choose **Services > Mobile Concierge**.
- Step 2** Choose **Mobile Concierge Services > Policies** from the left sidebar menu. The Policies page appears.
- Step 3** Select the check box of the policy that you want to delete.
- Step 4** From the Select a command drop-down list, choose **Delete Policy**, and click **Go**.
- Step 5** Click **OK** to confirm the deletion.
-



Managing Users and Groups

This chapter describes how to manage users, groups, and host access on the Cisco Mobility Services Engine.

- [Prerequisites, page 67](#)
- [Guidelines and Limitations, page 67](#)
- [Managing User Groups, page 67](#)
- [Managing Users, page 69](#)

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.

- [Adding User Groups](#)
- [Deleting User Groups](#)
- [Changing User Group Permissions](#)

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**.
- Step 2** Click the name of the MSE 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 MSEs.
- 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**.
- 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 a user with full access is added to a group that has only read access, that user will not be able to configure mobility services engine settings.

To change user group permissions, follow these steps:

-
- Step 1** Choose **Services > Mobility Services**.
 - Step 2** Click the name of the mobility services engine you want to edit.
 - Step 3** Choose **System > Accounts > Groups**.
 - Step 4** Click the name of the group you want to edit.
 - Step 5** From the Permission drop-down list, choose a permission level (**read, write, 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.

- [Adding Users](#)
- [Deleting Users](#)
- [Changing User Properties](#)

Adding Users

**Caution**

Group permissions override individual user permissions. For example, if a user with full access is added to a group that has only read access, that user will not be able to configure mobility services engine settings.

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

-
- Step 1** Choose **Services > Mobility Services Mobility Services Engines**.
 - Step 2** Click the name of the MSE 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** Re-enter 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 Prime Infrastructure to access MSEs.

Step 10 Click **Save**.

Deleting Users

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

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

Changing User Properties

To change user properties, follow these steps:

-
- Step 1** Launch the MSE admin UI.
 - Step 2** Click the Configuration icon on the top right of the home page.
 - Step 3** Choose **System > Accounts > Users**.
 - Step 4** Click the name of the user that you want to edit.
 - Step 5** Make the required changes to the **Password and Group Name** text boxes.
 - Step 6** Click **Save**.
-



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 Cisco 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 7.3.101.0.

- [Information About Event Notifications](#), page 71
- [Adding and Deleting Event Groups](#), page 76
- [Adding, Deleting, and Testing event Definitions](#), page 77
- [Prime Infrastructure as a Notification Listener](#), page 80

Information About Event Notifications

- Event Group—Helps you organize 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)
 - Simple Network Management Protocol (SNMP)
 - Syslog
- [Viewing Event Notification Summary](#), on page 72

- [Clearing Notifications](#), on page 72
- [Notification Message Formats](#), on page 73

Viewing Event Notification Summary

The mobility services engine sends event notifications and does not store them. However, if 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 MSE generates an absence event when an asset goes missing. In other words, the MSE cannot detect the asset in the WLAN for the specified time.
- **In/Out Area (Containment)**—The MSE 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) using **Monitor > Maps**. You can define a coverage area using the Map Editor.

- **Movement from Marker (Movement/Distance)**—The MSE 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 MSE generates location change events when a client station, asset tag, rogue client, or rogue access point changes its location.
- **Battery Level**—The MSE generates battery level events for all tracked asset tags.
- **Emergency**—The MSE 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 MSE 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 MSE.

Clearing Notifications

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

Notification Message Formats

- [Notification Formats in XML](#), on page 73
- [Notification Formats in Text](#), on page 73

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.

Notification Formats in XML

- [Missing \(Absence\) Condition](#), on page 74
- [In/Out \(Containment\) Condition](#), on page 74
- [Distance Condition](#), on page 75
- [Battery Level](#), on page 75
- [Location Change](#), on page 75
- [Chokepoint Condition](#), on page 75
- [Emergency Condition](#), on page 75

**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 quality 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.

Adding and Deleting Event Groups



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

- [Adding Event Groups, on page 76](#)
- [Deleting Event Groups, on page 76](#)

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**, and then Click **Go**.
 - Step 5** Click **OK** to confirm deletion.
 - Step 6** Click **Save**.
-

Adding, Deleting, and Testing event Definitions

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

- [Adding an Event Definition, on page 77](#)
- [Deleting an Event Definition, on page 79](#)
- [Testing Event Definitions, on page 79](#)

Adding an Event Definition

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** At 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:
- 1 Click **Add** to add a condition that triggers a notification.
 - 2 In the Add/Edit Condition dialog box, follow these steps:
 - a 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 MSE 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 MSE about it, or if the MSE does not hear anything about this device from the controller for 60 minutes by default. This value is 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 [Adding an Event Definition](#).
 - 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 [Adding an Event Definition](#).

- 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 [Adding an Event Definition](#).

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 [Adding an Event Definition](#).
- If you chose Location Change from the Condition Type drop-down list, proceed to Step [Adding an Event Definition](#).
- 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 [Adding an Event Definition](#).
- If you chose Chokepoint from the Condition Type drop-down list, proceed to Step [Adding an Event Definition](#). There is only one trigger condition and it is displayed by default. No configuration required.

3 In the Trigger If text box, specify the time in minutes to trigger the notification. The default is 60 minutes.

4 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.

5 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.

6 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 Prime Infrastructure.

- 7 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.

Deleting an Event Definition

To delete one or more event definitions from the Prime Infrastructure, follow these steps:

-
- Step 1** Choose **Services > Context Aware Notifications**.
 - Step 2** Choose **Notification Definitions**.
 - Step 3** Click the name of the group from which you want to delete an event definition.
 - Step 4** Select the event definition that you want to delete by selecting its corresponding check box.
 - Step 5** From the Select a command drop-down list, choose **Delete Event Definition(s)**, and then click **Go**.
 - Step 6** Click **OK** to confirm that you want to delete the selected event definition.
-

Testing Event Definitions

To test one or more event notifications of an event definition, follow these steps:

-
- Step 1** Choose **Services > Context Aware Notifications**.
 - Step 2** Choose **Notification Settings**.
 - Step 3** Click the name of the group containing the event definitions that you want to test.
 - Step 4** Select the event definitions that you want to test by selecting their corresponding check boxes.
 - Step 5** From the Select a command drop-down list, choose **Test-Fire Event Definition(s)**, and then click **Go**.
 - Step 6** Click **OK** to confirm that you want to test the event notifications.
 - Step 7** Ensure that notifications were sent to the designated recipient.
-

Prime Infrastructure as a Notification Listener

Prime Infrastructure acts as a notification listener. It 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

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



Context-Aware Service Planning and Verification

This chapter contains the following sections:

- [Licensing Requirement, page 81](#)
- [Planning Data, Voice, and Location Deployment, page 81](#)
- [Calibration Models, page 83](#)
- [Inspecting Location Readiness and Quality, page 85](#)
- [Verifying Location Accuracy, page 87](#)
- [Using Optimized Monitor Mode to Enhance Tag Location Reporting, page 90](#)
- [Configuring Interferer Notification, page 91](#)
- [Modifying Context-Aware Service Parameters, page 92](#)
- [Enabling Notifications and Configuring Notification Parameters, page 105](#)
- [Location Template for Cisco Wireless LAN Controllers, page 108](#)
- [Location Services on Wired Switches and Wired Clients, page 111](#)
- [Verifying an NMSP Connection to a Mobility Services Engine, page 115](#)

Licensing Requirement

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

Planning Data, Voice, and Location Deployment

This section contains the following topics:

- [Guidelines and Limitations, on page 82](#)

- [Calculating the Placement of Access Points](#), on page 82

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 seven 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 > 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 placements 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

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.
- [Guidelines and Limitations for Calibration Model](#), on page 83
- [Creating and Applying Data Point and Calibration Models](#), on page 83

Guidelines and Limitations for Calibration Model

- 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 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**, and then 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**, and then 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 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 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.
- 1 To perform a point collection, follow these steps:
 - a 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.
 - b 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.
 - c 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.
 - d Repeat point collection Steps ai to aiii 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.

- 2 To perform a linear collection, follow these steps:
 - a 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.
 - b Position the tip of the Start pop-up at the starting data point.
 - c Position the Finish pop-up at the ending data point.
 - d 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.
 - e 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).
 - f Repeat Steps bii to bv 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.
- 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

This section contains the following topics:

- [Guidelines and Limitations, on page 86](#)
- [Inspecting Location Quality Using Calibration Data, on page 86](#)
- [Inspecting Location Readiness Using Access Point Data, on page 86](#)

Guidelines and Limitations

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 the 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 in the Floor Settings menu.
- Note** If clients, 802.11 tags, access points, and interferers are not displayed, verify that their respective check boxes are selected in the Floor Settings menu. Additionally, licenses for both clients and tags must be purchased for each of them to be tracked.
- Note** See [Adding and Deleting Mobility Services Engines and Licenses, on page 7](#) 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, 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 data, follow these steps:

-
- Step 1** Choose **Monitor > Site Maps**.
- Step 2** From the Select a command drop-down list, choose **RF Calibration Model**, and then 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.

- [Using Scheduled Accuracy Testing to Verify Current Location Accuracy, on page 87](#)
- [Using On-Demand Location Accuracy Testing, on page 88](#)

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**.
- Note** The campus, building, and floors displayed on this page are filtered based on virtual domain.
- Step 3** Enter a test name.
- Step 4** Choose an area type from the drop-down list.
- Note** Campus is configured as system campus by default. There is no need to change this setting.

- Step 5** Choose the building from the drop-down list.
- Step 6** Choose the floor from the drop-down list.
- Step 7** 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 8** 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 9** Click **Position Testpoints**. The floor map appears with a list of all clients and tags on that floor with their MAC addresses.
- Step 10** 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 11** 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 12** Click **Save** when all elements are positioned. A page appears confirming successful accuracy testing.
- Step 13** 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 14** To view the results of the location accuracy test, click **Test name** and then click **Download** in the page that appears. 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.
Note Campus is configured as system campus by default. There is no need to change this setting.
- Step 5** Choose the building from the drop-down list.
- Step 6** Choose the floor from the drop-down list.
- Step 7** View the test results in the Accuracy Tests > Results page. Reports are in PDF format.
- Step 8** Click **Position Testpoints**. The floor map appears with red cross hairs at the (0,0) coordinate.
- Step 9** 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 10** 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 11** Click **Start** to begin collecting accuracy data.
- Step 12** Click **Stop** to finish collecting data.
Note You should allow the test to run for at least two minutes before clicking Stop.
- Step 13** Repeat Step 10 to Step 13 for each testpoint that you want to plot on the map.
- Step 14** Click **Analyze** when you are finished mapping the testpoints.
- Step 15** 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 16** To download accuracy test logs from the Accuracy Tests summary page:
- 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.
 - 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 Tracking Optimized Monitor Mode (TOMM) 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.

- [Guidelines and Limitations](#), on page 90
- [Optimizing Monitoring and Location Calculation of Tags](#), on page 90

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.
- 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 deselecting 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.
 - Click **Save**.
 - In the Radio parameters page, re-enable the radio by selecting the **Admin Status** check box.
 - 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.
-

Configuring Interferer Notification

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 Trasmmitter
- Jammer
- Continous Transmitter
- DECT like Phone
- Video Camera
- 80.15.4
- 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**.

Modifying Context-Aware Service Parameters

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.

- [Licensing Requirement](#), on page 81
- [Guidelines and Limitations](#), on page 92
- [Modifying Tracking Parameters](#), on page 92
- [Modifying Filtering Parameters](#), on page 96
- [Modifying History Parameters](#), on page 98
- [Enabling Location Presence](#), on page 100
- [Importing and Exporting Asset Information](#), on page 101
- [Modifying Location Parameters](#), on page 102

Licensing Requirement

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 25k for Cisco 3355 Mobility Service Engine and upto 50000 clients for Virtual Appliance (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 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 25,000 trackable units, you can set a limit to track only 10,000 client stations (leaving 15,000 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 includes the following topics:

- [Guidelines and Limitations](#), on page 93
- [Configuring Tracking Parameters for a Mobility Services Engine](#), on page 93

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**. The Mobility Services page appears.
 - Step 2** Click the name of the MSE 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. The following table lists the tracking parameters.

Table 8: Tracking Parameters

Field	Configuration Options
Tracking Parameters	

Field	Configuration Options
Wired Clients	<p>1 Select the Enable check box to enable tracking of client stations by the MSE.</p> <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 MSE 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> <p>Caution When upgrading the MSE 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	<p>1 Select the Enable check box to enable tracking of client stations by the MSE.</p> <p>2 Select the Enable Limiting check box to set a limit on the number of client stations to track.</p> <p>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 clients that can be tracked by a MSE.</p> <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>
Rogue Access Points	<p>1 Select the Enable check box to enable tracking of rogue access points by the MSE.</p> <p>2 Select the Enable Limiting check box to set a limit on the number of rogue access points to track.</p> <p>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 MSE.</p> <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	<p>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.</p>

Field	Configuration Options
Rogue Clients	<ol style="list-style-type: none"> 1 Select the Enable check box to enable tracking of rogue clients by the MSE. 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. This limit varies based on the platform. The limit value is the maximum number of rogue clients that can be tracked by a MSE. <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 MSE. 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	
Active RFID Tags	<p>Select the Enable check box to enable tracking of active RFID tags by the MSE.</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 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).

Field	Configuration Options
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	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. Note Before the mobility service can collect asset tag data from Cisco WLCs, you must enable the detection of active RFID tags using the config rfid status enable command on the Cisco WLCs.
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. 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 MSE database.

Modifying Filtering Parameters

- 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 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.

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.

Modifying Filtering Parameters contains the following topics:

- [Guidelines and Limitations](#), on page 97
- [Configuring Filtering Parameters for a Mobility Services Engine](#), on page 97

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. The following table lists filtering parameters.

Table 9: Filtering Parameters

Field	Configuration Options
Advanced Filtering Parameters	
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 choose to specify a filter for interferers based on the duty cycle of the interferer.</p>

Field	Configuration Options
RSSI Cutoff for Probing Clients	Enter the RSSI cutoff value for probing clients so that those clients whose RSSI values are below the cutoff value is reported. The default value for the RSSI cutoff for probing clients is -128dB.
MAC Filtering Parameters	
Exclude Probing Clients	Select the check box to prevent calculating location for probing clients.
Enable Location MAC Filtering	<ol style="list-style-type: none"> Select the check box to enable filtering of specific elements by their MAC addresses. 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. <ul style="list-style-type: none"> Note To view allowed MAC address formats, click the red question mark next to the Upload a file for Location MAC Filtering text box. To add an individual MAC address, enter the MAC addresses (format is xx:xx:xx:xx:xx:xx) and click either Allow or Disallow. The address appears in the appropriate column. <ul style="list-style-type: none"> Note To move an address between the Allow and Disallow columns, highlight the MAC address entry and click the button under the appropriate column. 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. 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.

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

Modifying History Parameters

This section contains the following topics:

- [Guidelines and Limitations](#), on page 99
- [Configuring Mobility Services Engine History Parameters](#), on page 99

Guidelines and Limitations

Before enabling location presence, synchronize the mobility services engine.

Configuring Mobility Services Engine History Parameters

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. The following table lists history parameter.

Table 10: 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 Cisco WLC, 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, you have to synchronize the mobility services engine.

- [Guidelines and Limitations](#), on page 99
- [Enabling and Configuring Location Presence on a Mobility Services Engine](#), on page 100

Guidelines and Limitations

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 MSE 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 MSE returns the client address as *Building A*.
 - b) When AP is selected, the MSE 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 MSE returns the client address of *3034:00hh:0adg*.
 - c) When X,Y is selected, the MSE 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 MSE 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, on page 101](#)
- [Exporting Asset Information, on page 102](#)

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** in the dialog box when download is complete.
-

Modifying Location Parameters

This section contains the following topic:

- [Configuring Location Parameters, on page 102](#)

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. The following table lists location parameters.

Table 11: Location Parameters

Field	Configuration Options
Enable Calculation time	Select the Enable check box to initiate the calculation of the time required to compute location. Note This parameter applies only to clients, rogue access points, rogue clients, and interferers. Caution Enable this parameter only under Cisco TAC personnel guidance because it slows down the overall location calculations.
Enabled OW Location	Select the Enable check box to include Outer Wall (OW) calculation as part of location calculation. Note This parameter is ignored by the MSE.
Relative discard RSSI time	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 MSE 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. Note This parameter applies only to clients, rogue access points, rogue clients, and interferers.
Absolute discard RSSI time	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. Note This parameter applies only to clients.
RSSI Cutoff	Enter the RSSI cutoff value, in decibels (dBs) with respect to one (1) mW (dBm), above which the MSE will always use the access point measurement. The default value is -75. Note When 3 or more measurements are available above the RSSI cutoff value, the MSE 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. Note This parameter applies only to clients. Caution Modify only under Cisco TAC personnel guidance. Modifying this value can reduce the accuracy of location calculation.
Enable Location Filtering	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.

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.

Step 5 Click Save.

Enabling Notifications and Configuring Notification Parameters

This section contains the following topics:

- [Enabling Notifications](#), on page 105
- [Configuring Notification Parameters](#), on page 105
- [Viewing Notification Statistics](#), on page 107

Enabling Notifications

User-configured conditional notifications manage which notifications the mobility services engine sends to Prime Infrastructure or a third-party destination compatible with the mobility services engine notifications.

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 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 within a certain period.

Notification parameter settings apply to user-configurable conditional notifications and northbound notifications except as noted in [Configuring Notification Parameters](#), on page 105.



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**.
- 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 page. The following table describes the user-configurable conditional and northbound notifications fields.

Table 12: 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).

Field	Configuration Options
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 3310 (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.
Refresh Time	Enter the wait time in minutes that must pass before a notification is re-sent. 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**.

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, choose **Services > Mobility Services > MSE-name > Context Aware Service > Notification Statistics**.

where *MSE-name* is the name of a mobility services engine.

The following table lists fields in the Notification Statistics page.

Table 13: Notification Statistics Page

Field	Description
Summary	
Destinations	
Total	Destinations total count.
Unreachable	Unreachable destinations 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.
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 Cisco Wireless LAN 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.

This section contains [Configuring a New Location Template for a Wireless LAN Controller](#), on page 110

FastLocate Overview

Current generation of Wi-Fi clients probe less frequently to conserve battery power. It is often the case that probing behavior of a Wi-Fi client is device dependent. This poses a challenge for all W-Fi based location solution because they rely on RSSI measurements from probe frames that can be heard by multiple APs. With fewer probes from Wi-Fi clients, location updates become infrequent. Cisco has introduced FastLocate technology that addresses this problem. FastLocate makes it possible for multiple APs to hear the data packets at the same time. This is achieved with Wireless Security Module (WSM) to collect data packet RSSI sent by the associated Wi-Fi clients. Unlike probe request frames, applications on smartphone easily generate data traffic when they are connected to the Wi-Fi network. Enabling this feature will increase the update rate of location for all associated clients leading to a smoother blue dot experience. FastLocate increased the locate updates with minimal impact on clients battery life and is also device independent.

Deployment Considerations

- FastLocate technology does not require new hardware or AP. The existing WSM module with AP 3K can be used.
- FastLocate and advanced security monitoring can be simultaneously turned ON.
- MSE location algorithms can simultaneously calculate location from probes and data RSSI. There is no need to dedicate a new MSE for FastLocate.
- For best results, all APs in the RF environment will have WSM module. This is a 1:1 density of APs with WSM module. While a mix of APs with module and without modules is possible, this deployment needs to be carefully planned. This is not a recommended deployment at this time.
- Enabling FastLocate provides limited improvement on the update rate of unassociated clients.
- Since data packets are more frequent, using data packets for location increases the computation burden at the MSE Location engine. This has an impact on the total number of simultaneous active clients that can be tracked by the MSE.
- A rule of thumb is to reduce the maximum number of clients tracked by a factor of 5. For example, high end virtual MSE that can track up to 50,000 devices using probes can track up to 10,000 devices using Data packets.

Configuring a New Location Template for a Wireless LAN Controller

- 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.
- Step 3** In the New Controller Template page, enter a name for the location template in the General tab
- Step 4** In the General tab, modify parameters as necessary. The following table lists General tab fields.

Table 14: General Tab Fields

Parameter	Configuration Options
RFID tag calculation	Select the Enabled check box to collect data on tags.
Calibrating Client	Select the Enabled check box to have a calibrating client. Cisco WLCs 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	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 Cisco WLCs 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 Cisco WLCs is synchronized with the mobility services engine, the new value is set on the mobility services engine.
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.
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.
The following table describes each of the Advanced tab fields.

Table 15: Advanced Location Fields

Field	Configuration Options
RFID Tag Data Timeout	Enter an RFID tag data timeout value.
Calibrating Client Multiband	Select the Enable 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

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 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>

- [Prerequisites to Support Location Services for Wired Clients](#), on page 111
- [Guidelines and Limitations](#), on page 112
- [Configuring a Catalyst Switch Using the CLI](#), on page 112
- [Adding a Catalyst Switch to Prime Infrastructure](#), on page 114
- [Assigning and Synchronizing a Catalyst Switch to a Mobility Services Engine](#), on page 114

Prerequisites to Support Location Services for Wired Clients

- Configure the Catalyst switch.
- Add the Catalyst switch to 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

- 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



Note All commands are located in the privileged EXEC mode of the command-line interface.

To configure location services on a wired switch or wired client, and apply it to an interface, follow these steps:

Step 1 Log in to the command-line interface of the switch:

```
Switch > enable
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 timer 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 Prime Infrastructure

All Catalyst switches must be configured with location services before they are added to Prime Infrastructure. To add a Catalyst switch configured for wired location service to Prime Infrastructure, follow these steps:

-
- Step 1** Choose **Configure > Ethernet Switches**.
- Step 2** From the Select a command drop-down list, choose **Add Ethernet Switches**. The Add Ethernet 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** Select the **Location Capable** check box.
- Step 6** From the drop-down list, choose the SNMP version if it is different from the default.
Note No changes are required in the Retries and Timeout text boxes.
- Step 7** Enter **wired-location** as the SNMP community string in the Community text box.
- Step 8** Click **Prime Infrastructure**. A page confirming the successful addition to Prime Infrastructure appears.
- Step 9** 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 MSE. However, a MSE can have many switches connected to it.

To assign and synchronize Catalyst switches to a MSE, follow these steps:

-
- Step 1** Choose **Services > Synchronize Services**.
- Step 2** Click the **Wired Switches** tab to assign a switch to a MSE.
- Step 3** Choose one or more switches to be synchronized with the MSE.
- Step 4** Click **Change MSE Assignment**.
- Step 5** Choose the MSE to which the switches are to be synchronized.
- Step 6** Click **Synchronize** to update the MSE(s) database(s).

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

- Step 7** To verify the NMSP connection between the switch and a MSE, see the [Verifying an NMSP Connection to a Mobility Services Engine](#), on page 115.
-

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 MSE 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 MSE.

Note On a Catalyst wired switch, enter the **show nmsp status** command to verify NMSP connection.



Working with Maps

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

- [About Maps, page 117](#)
- [Adding a Campus Map, page 123](#)
- [Configuring Buildings, page 123](#)
- [Adding Floor Areas, page 128](#)
- [Monitoring the Floor Area, page 146](#)
- [Using the Automatic Hierarchy to Create Maps, page 149](#)
- [Using the Map Editor, page 152](#)
- [Using Chokepoints to Enhance Tag Location Reporting, page 158](#)

About Maps

The Next Generation Maps feature is enabled by default.

The Next Generation Maps feature provides you the following benefits:

- Displays large amount of information on the map. When you have various clients, interferers, and access points, they may clutter the display on the Prime Infrastructure map pages and sometimes pages load slowly. The Release 7.3 introduces clustering and layering of information. Information cluster reduces clutter at the high level and reveals more information when you click an object. For details, see the [Monitoring the Floor Area, on page 146](#).
- Simplifies and accelerates the process of adding APs to the map. In the legacy maps, the process of adding access points to maps was manual and tedious. With Release 7.3, you can use the automated hierarchy creation to add and name the access points. For details, see the [Using the Automatic Hierarchy to Create Maps, on page 149](#).
- Provides high quality map images with easy navigation and zoom/pan controls. In the legacy maps, the map image quality was low and the navigating, zooming, and panning was slow. With Release 7.3, you can use the next-generation tile-aware map engine to load maps faster and zoom/pan easily. The Next

Generation Maps enables you to load high resolution maps faster and navigate around the map easily. For details, see the [Planning and Zooming with Next Generation Maps](#), on page 146.

- [Adding a Building to a Campus Map](#), on page 118
- [Adding Floor Areas](#), on page 119

Adding a Building to a Campus Map

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

-
- Step 1** Choose **Design > Site Maps** to display the Maps page.
- Step 2** Click the desired campus. The Site Maps > Campus Name page appears.
- Step 3** From the Select a command drop-down list, choose **New Building**, and click **Go**.
- Step 4** In the Campus Name > New Building page, follow these steps to create a virtual building in which you can organize related floor plan maps:
- 1 Enter the building name.
 - 2 Enter the building contact name.
 - 3 Enter the number of floors and basements.
 - 4 Enter the horizontal position (distance from the corner of the building rectangle to the left edge of the campus map) and the vertical position (distance from the corner of the building rectangle to the top edge of the campus map) in feet.

Note To change the unit of measurement (feet or meters), choose **Design > Site Maps**, and choose **Properties** from the Select a command drop-down list.
 - 5 Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.

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

Tip You can also use **Ctrl-click** to resize the bounding area in the upper-left corner of the campus map. As you change the size of the bounding area, the horizontal span and the vertical span parameters of the building change to match your actions.
 - 6 Click **Place** to put the building on the campus map. The Prime Infrastructure creates a building rectangle scaled to the size of the campus map.
 - 7 Click the building rectangle and drag it to the desired position on the campus map.

Note After adding a new building, you can move it from one campus to another without having to recreate it.
 - 8 Click **Save** to save this building and its campus location to the database. The Prime Infrastructure saves the building name in the rectangle on the campus map.

Note A hyperlink associated with the building takes you to the corresponding Map page.
- Step 5** (Optional) To assign location presence information for the new outdoor area, do the following:

- 1 Choose **Edit Location Presence Info** from the Select a command drop-down list. Click **Go**. The Location Presence page appears.
- 2 Click the **Civic Address** or **Advanced** tab.
 - Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
 - Advanced identifies the campus with expanded civic information such as neighborhood, city division, country, and postal community name.

Note Each selected field is inclusive of all of those above it. For example, if you choose Advanced, it can also provide civic location information upon client demand. The selected setting must match what is set on the location server level (Services > Mobility Services).
- 3 By default, the Override Child's Presence Information check box is selected. There is no need to alter this setting for standalone buildings.

Step 6 Click **Save**.

Adding Floor Areas

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

- [Adding Floor Areas to a Campus Building](#), on page 119
- [Adding Floor Plans to a Standalone Building](#), on page 121
- [Configuring Floor Settings](#), on page 132
- [Import Map and AP Location Data](#), on page 145

Adding Floor Areas to a Campus Building



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

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

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

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

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

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

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

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

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

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

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

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

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

1 Enter the floor area and contact names.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Enter the remaining parameters for the floor area.

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

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

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

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

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

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

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

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

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

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

Adding Floor Plans to a Standalone Building

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

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

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

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

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

Step 6 Click **Go**.

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

- Enter the floor area and contact names.
- Choose the floor or basement number from the Floor drop-down list.
- Choose the floor or basement type (RF Model).
- Enter the floor-to-floor height in feet
- Select the **Image or CAD File** check box.
- Browse to and choose the desired floor or basement Image or CAD file, and click **Open**.

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

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

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

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

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

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

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

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

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

Step 9 Enter the remaining parameters for the floor area.

- Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio
- Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

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

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

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

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

- Step 10** Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Design > Site Maps list.
- Step 11** Click any of the floor or basement images to view the floor plan or basement map.
- Note** You can zoom in or out to view the map at different sizes and you can add access points.
-

Adding a Campus Map

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

-
- Step 1** Save the map in .PNG, .JPG, .JPEG, or .GIF format.
- Note** The map can be of any size because the Prime Infrastructure automatically resizes the map to fit the working areas.
- Step 2** Browse to and import the map from anywhere in your file system.
- Step 3** Choose **Design > Site Maps** to display the Maps page.
- Step 4** From the Select a command drop-down list, choose **New Campus**, and click **Go**.
- Step 5** In the Maps > New Campus page, enter the campus name and campus contact name.
- Step 6** Browse to and choose the image filename containing the map of the campus, and click **Open**.
- Step 7** Select the **Maintain Aspect Ratio** check box to prevent length and width distortion when the Prime Infrastructure resizes the map.
- Step 8** Enter the horizontal and vertical span of the map in feet.
- Note** To change the unit of measurement (feet or meters), choose **Design > Site Maps** and choose **Properties** from the Select a command drop-down list. The horizontal and vertical span should be larger than any building or floor plan to be added to the campus.
- Step 9** Click **OK** to add this campus map to the Prime Infrastructure database. The Prime Infrastructure displays the Maps page, which lists maps in the database, map types, and campus status.
- Step 10** (Optional) To assign location presence information, click the newly created campus link in the Design > Site Maps page.
-

Configuring Buildings

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

- [Adding a Building to a Campus Map](#), on page 209

- [Viewing a Building, on page 126](#)
- [Editing a Building, on page 127](#)
- [Deleting a Building, on page 127](#)
- [Moving a Building, on page 128](#)

Adding a Building to a Campus Map

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

-
- Step 1** Choose **Monitor > Site Maps** to display the Maps page.
- Step 2** Click the desired campus. The Site Maps > Campus Name page appears.
- Step 3** From the Select a command drop-down list, choose New Building, and click **Go**.
- Step 4** In the Campus Name > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:
- a) Enter the building name.
 - b) Enter the building contact name.
 - c) Enter the number of floors and basements.
 - d) Enter the horizontal position (distance from the corner of the building rectangle to the left edge of the campus map) and the vertical position (distance from the corner of the building rectangle to the top edge of the campus map) in feet.

Note To change the unit of measurement (feet or meters), choose Monitor > Site Maps, and choose Properties from the Select a command drop-down list.
 - e) Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.

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

Tip You can also use Ctrl-click to resize the bounding area in the upper-left corner of the campus map. As you change the size of the bounding area, the Horizontal Span and Vertical Span parameters of the building change to match your actions.
 - f) Click **Place** to put the building on the campus map. The NCS creates a building rectangle scaled to the size of the campus map.
 - g) Click the building rectangle and drag it to the desired position on the campus map.

Note After adding a new building, you can move it from one campus to another without having to recreate it.
 - h) Click **Save** to save this building and its campus location to the database. The NCS saves the building name in the building rectangle on the campus map.

Note A hyperlink associated with the building takes you to the corresponding Map page.
- Step 5** (*Optional*) To assign location presence information for the new outdoor area, do the following:
- a) Choose **Edit Location Presence Info** from the Select a command drop-down list. Click **Go**. The Location Presence page appears.

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

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

- Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
- GPS Markers identify the campus by longitude and latitude.
- Advanced identifies the campus with expanded civic information such as neighborhood, city division, country, and postal community name.

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

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

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

Step 6 Click **Save**.

Adding a Standalone Building

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

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

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

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

a) Enter the building name.

b) Enter the building contact name.

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

c) Enter the number of floors and basements.

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

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

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

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

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

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

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

- Civic Address identifies the campus by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
- GPS Markers identify the campus by longitude and latitude.
- Advanced identifies the campus with expanded civic information such as neighborhood, city division, county, and postal community name.

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

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

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

Step 5 Click **Save**.

Note The standalone buildings are automatically placed in System Campus.

Viewing a Building

To view a current building map, follow these steps:

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

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

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

The map details include the following:

- Floor area
- Floor index—Indicates the floor level. A negative number indicates a basement floor level.
- Contact
- Status—Indicates the most serious level of alarm on an access point located on this map or one of its children.
- Number of total access points located on the map.
- Number of 802.11a/n and 802.11b/g/n radios located on the map.
- Number of out of service (OOS) radios.
- Number of clients—Click the number link to view the Monitor > Clients page.

- Step 3** The Select a command drop-down list provides the following options:
- New Floor Area—See the [Adding a Building to a Campus Map, on page 209](#) for more information.
 - Edit Building—See the [Editing a Building, on page 127](#) for more information.
 - Delete Building—See the [Deleting a Building, on page 127](#) for more information.
-

Editing a Building

To edit a current building map, follow these steps:

-
- Step 1** Choose **Monitor > Site Maps**.
- Step 2** Click the name of the building map to open its details page.
- Step 3** From the Select a command drop-down list, choose **Edit Building**.
- Step 4** Make any necessary changes to Building Name, Contact, Number of Floors, Number of Basements, and Dimensions (feet).
- Note** To change the unit of measurement (feet or meters), choose **Monitor > Site Maps**, and choose **Properties** from the Select a command drop-down list.
- Step 5** Click **OK**.
-

Deleting a Building

To delete a current building map, follow these steps:

-
- Step 1** Choose **Monitor > Site Maps**.
- Step 2** Select the check box for the building that you want to delete.
- Step 3** Click **Delete** at the bottom of the map list (or choose **Delete Maps** from the Select a command drop-down list, and click **Go**).
- Step 4** Click **OK** to confirm the deletion.
- Note** Deleting a building also deletes all of its container maps. The access points from all deleted maps are moved to an Unassigned state.
-

Moving a Building

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

-
- Step 1** Choose **Monitor > Site Maps**.
 - Step 2** Select the check box of the applicable building.
 - Step 3** From the Select a command drop-down list, choose **Move Buildings**.
 - Step 4** Click **Go**.
 - Step 5** Choose the **Target Campus** from the drop-down list.
 - Step 6** Select the buildings that you want to move. Unselect any buildings that remain in their current location.
 - Step 7** Click **OK**.
-

Adding Floor Areas

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

- [Adding Floor Areas to a Campus Building](#), on page 119
- [Adding Floor Plans to a Standalone Building](#), on page 121
- [Configuring Floor Settings](#), on page 132
- [Import Map and AP Location Data](#), on page 145

Adding Floor Areas to a Campus Building



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

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

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

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

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

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

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

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

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

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

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

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

1 Enter the floor area and contact names.

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

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

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

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

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

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

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

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

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

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

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

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

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

- Note** The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.
- 8 If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.
- Enter the remaining parameters for the floor area.
- 9 Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.
- 10 Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.
- Note** The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure database.
- 11 If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.
- Tip** Use **Ctrl-click** to resize the image within the building-sized grid.
- 12 If desired, select the **Launch Map Editor after floor creation** check box to rescale the floor and draw walls.
- 13 Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Design > Site Maps list.
- Note** Use different floor names in each building. If you are adding more than one building to the campus map, do not use a floor name that exists in another building. This overlap causes incorrect mapping information between a floor and a building.
- 14 Click any of the floor or basement images to view the floor plan or basement map.
- Note** You can zoom in or out to view the map at different sizes and you can add access points.
-

Adding Floor Plans to a Standalone Building

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

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

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

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

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

Step 6 Click **Go**.

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

- Enter the floor area and contact names.
- Choose the floor or basement number from the Floor drop-down list.
- Choose the floor or basement type (RF Model).
- Enter the floor-to-floor height in feet
- Select the **Image or CAD File** check box.
- Browse to and choose the desired floor or basement Image or CAD file, and click **Open**.

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

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

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

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

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

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

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

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

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

Step 9 Enter the remaining parameters for the floor area.

- Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio
- Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

Note The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure Prime Infrastructure database.
- If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

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

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

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

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

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

Configuring Floor Settings

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



Note

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

The Floor Settings options include the following:

- Access Points—See the [Filtering Access Point Floor Settings](#) for more information.
- AP Heatmaps—See the [Filtering Access Point Heatmap Floor Settings](#) for more information.
- AP Mesh Info—See the [Filtering AP Mesh Info Floor Settings](#) for more information.
- Clients—See the [Filtering Client Floor Settings](#) for more information.
- 802.11 Tags—See the [Filtering 802.11 Tag Floor Settings](#) for more information.
- Rogue APs—See the [Filtering Rogue AP Floor Settings](#) for more information.
- Rogue Adhocs—See the [Filtering Rogue Adhoc Floor Settings](#) for more information.
- Rogue Clients—See the [Filtering Rogue Client Floor Settings](#) for more information.
- Coverage Areas
- Location Regions
- Rails
- Markers
- Chokepoints
- Wi-Fi TDOA Receivers
- Interferers—See the [Filtering Interferer Settings](#) for more information.
- wIPS Attackers—See the [Filtering wIPS Attacker Floor Settings](#), on page 143 for more information.

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

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

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

Defining Inclusion and Exclusion Regions on a Floor

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

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

Cisco 1000 Series Lightweight Access Point Icons

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















Note


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

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

Table 16: Access Points Icons Description

Icon	Description
	The green icon indicates an access point (AP) with no faults. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio.
	The yellow icon indicates an access point with a minor fault. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio. Note A flashing yellow icon indicates that there has been an 802.11a or 802.11b/g interference, noise, coverage, or load Profile Failure. A flashing yellow icon indicates that there have been 802.11a and 802.11b/g profile failures.
	The red icon indicates an access point (AP) with a major or critical fault. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio.



Icon	Description
	The dimmed icon with a question mark in the middle represents an unreachable access point. It is gray because its status cannot be determined.
	The dimmed icon with no question mark in the middle represents an unassociated access point.
	The icon with a red "x" in the center of the circle represents an access point that has been administratively disabled.
	The icon with the top half green and the lower half yellow indicates that the optional 802.11a Cisco Radio (top) has no faults, and the 802.11b/g Cisco Radio (bottom) has a minor fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half green and the lower half red indicates that the optional 802.11a Cisco Radio (top) is operational with no faults, and the 802.11b/g Cisco Radio (bottom) has a major or critical fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half yellow and the lower half red indicates that the optional 802.11a Cisco Radio (top) has a minor fault, and the 802.11b/g Cisco Radio (bottom) has a major or critical fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half yellow and the lower half green indicates that the optional 802.11a Cisco Radio (top) has a minor fault, and the 802.11b/g Cisco Radio (bottom) is operational with no faults. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half red and the lower half green indicates that the optional 802.11a Cisco Radio (top) has a major or critical fault, and the 802.11b/g Cisco Radio (bottom) is operational with no faults. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.
	The icon with the top half red and the lower half yellow indicates that the optional 802.11a Cisco Radio (top) has major or critical faults, and the 802.11b/g Cisco Radio (bottom) has a minor fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.


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

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

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

Table 17: Arrows

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

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

Filtering Access Point Floor Settings

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

Access point filtering options include the following:

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



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

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



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

- Display—From the drop-down list, choose what identifying information is displayed for the access points on the map image.
 - Channels—Displays the Cisco Radio channel number or Unavailable (if the access point is not connected).



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

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

**Note**

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

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

Table 18: Transmit Power Level Values

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

**Note**

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

- Channel and Tx Power—Displays both the channel and transmit power level (or Unavailable if the access point is not connected).
- Coverage Holes—Displays a percentage of clients whose signal has become weaker until the client lost its connection, Unavailable for unconnected access points, or MonitorOnly for access points in monitor-only mode.

**Note**

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

- **MAC Addresses**—Displays the MAC address of the access point, whether or not the access point is associated to a controller.
- **Names**—Displays the access point name. This is the default value.
- **Controller IP**—Displays the IP address of the controller to which the access point is associated or Not Associated for disassociated access points.
- **Utilization**—Displays the percentage of bandwidth used by the associated client devices (including receiving, transmitting, and channel utilization). Displays Unavailable for disassociated access points and MonitorOnly for access points in monitor-only mode.
- **Profiles**—Displays the load, noise, interference, and coverage components of the corresponding operator-defined thresholds. Displays Okay for thresholds not exceeded, Issue for exceeded thresholds, or Unavailable for unconnected access points.



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

- **CleanAir Status**—Displays the CleanAir status of the access point and whether or not CleanAir is enabled on the access point.
- **Average Air Quality**—Displays the average air quality on this access point. The details include the band and the average air quality.
- **Minimum Air Quality**—Displays the minimum air quality on this access point. The details include the band and the minimum air quality.
- **Average and Minimum Air Quality**—Displays the average and minimum air quality on this access point. The details include the band, average air quality, and minimum air quality.
- **Associated Clients**—Displays the number of associated clients, Unavailable for unconnected access points or MonitorOnly for access points in monitor-only mode.



Note

- **Bridge Group Names**
- **RSSI Cutoff**—From the drop-down list, choose the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBm.
- **Show Detected Interferers**—Select the check box to display all interferers detected by the access point.
- **Max. Interferers/label**—Choose the maximum number of interferers to be displayed per label from the drop-down list.

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

Filtering Access Point Heatmap Floor Settings

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

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

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

Access point heatmap filtering options include the following:

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



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



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

- **Total APs**—Displays the number of access points positioned on the map.
- Select the access point check box(es) to determine which heatmaps are displayed on the image map.

Click OK when all applicable filtering criteria are selected.

Filtering AP Mesh Info Floor Settings



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

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

- Link between the child and the parent access point.
- An arrow that indicates the direction from the child to parent access point.
- A color-coded link that indicates the signal-to-noise ratio (SNR). A green link represents a high SNR (above 25 dB), an amber link represents an acceptable SNR (20-25 dB), and a red link represents a very low SNR (below 20 dB).

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

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



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

Click OK when all applicable filtering criteria are selected.

Filtering Client Floor Settings



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

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

Client filtering options include the following:

- Show All Clients—Select the check box to display all clients on the map.
- Small Icons—Select the check box to display icons for each client on the map.



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

- Display—Choose the client identifier (IP address, username, MAC address, asset name, asset group, or asset category) to display on the map.
- Filter By—Choose the parameter by which you want to filter the clients (IP address, username, MAC address, asset name, asset group, asset category, or controller). Once selected, type the specific device in the text box.
- SSID—Enter the client SSID in the available text box.
- Protocol—Choose All, 802.11a/n, or 802.11b/g/n from the drop-down list.
 - All—Displays all the access points in the area.
 - 802.11a/n—Displays a colored overlay depicting the coverage patterns for the clients with 802.11a/n radios. The colors show the received signal strength from red (–35 dBm) through dark blue (–85 dBm).
 - 802.11b/g/n—Displays a colored overlay depicting the coverage patterns for the clients with 802.11b/g/n radios. The colors show the received signal strength from red (–35 dBm) through dark blue (–85 dBm). This is the default value.
- State—Choose All, Idle, Authenticated, Probing, or Associated from the drop-down list.

Click OK when all applicable filtering criteria are selected.

Filtering 802.11 Tag Floor Settings

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

Tag filtering options include the following:

- Show All Tags—Select the check box to display all tags on the map.
- Small Icons—Select the check box to display icons for each tag on the map.

**Note**

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

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

Click OK when all applicable filtering criteria are selected.

Filtering Rogue AP Floor Settings

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

Rogue AP filtering options include the following:

- Show All Rogue APs—Select the check box to display all rogue access points on the map.
- Small Icons—Select the check box to display icons for each rogue access point on the map.

**Note**

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

- Show Rogue AP Zone of Impact—Select the check box to display the zone of impact for rogues. The rogue impact zone is determined by the transmission power of the Rogue AP and the number of clients associated with the rogue AP.
 - The number of clients associated with the rogue AP determines the intensity of the color of the zone on the map.
 - The radius of the zone of impact is determined by using the following transmission powers of the rogue AP.

Table 19: Transmission Powers

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

- **MAC Address**—If you want to view a particular MAC address, enter it in the MAC Address text box.
- **State**—Use the drop-down list to choose from Alert, Known, Acknowledged, Contained, Threat, or Unknown contained states.
- **On Network**—Use the drop-down list to specify whether or not you want to display rogue access points on the network.

Click OK when all applicable filtering criteria are selected.

Filtering Rogue Adhoc Floor Settings

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

Rogue Adhoc filtering options include the following:

- **Show All Rogue Adhocs**—Select the check box to display all rogue adhoc on the map.
- **Small Icons**—Select the check box to display icons for each rogue adhoc on the map.



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

- **MAC Address**—If you want to view a particular MAC address, enter it in the MAC Address text box.
- **State**—Use the drop-down list to select from Alert, Known, Acknowledged, Contained, Threat, or Unknown contained states.
- **On Network**—Use the drop-down list to specify whether or not you want to display rogue adhocs on the network.

Click OK when all applicable filtering criteria are selected.

Filtering Rogue Client Floor Settings

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

Rogue Clients filtering options include the following:

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

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



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

- **Assoc. Rogue AP MAC Address**—If you want to view a particular MAC address, enter it in the **MAC Address** text box.
- **State**—Use the drop-down list to choose from **Alert**, **Contained**, **Threat**, or **Unknown** contained states.

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

Filtering Interferer Settings

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

Interferer filtering options include the following:

- **Show active interferers only**—Select the check box to display all active interferers.
- **Small Icons**—Select the check box to display icons for each interferer on the map.
- **Show Zone of Impact**—Displays the approximate interference impact area. The opacity of the circle denotes its severity. A solid red circle represents a very strong interferer that likely disrupts Wi-Fi communications, a light pink circle represents a weak interferer.
- Click **OK** when all applicable filtering criteria are selected.

Filtering wIPS Attacker Floor Settings

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

wIPS Attack filtering options include the following:

- **Show All wIPS Attacks**—Select the check box to display all wIPS attacks on the map.
- **Small Icons**—Select the check box to display icons for each wIPS attacks on the map.



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

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

- MAC Address—If you want to view a particular MAC address, enter it in the MAC Address text box.
- Alarm Category—Choose the category of the alarm from the Alarm Category drop-down list. The possible categories are: **All Types, Security Penetration, User Authentication and Encryption, DoS, Performance Violation and Channel or Device overload.**

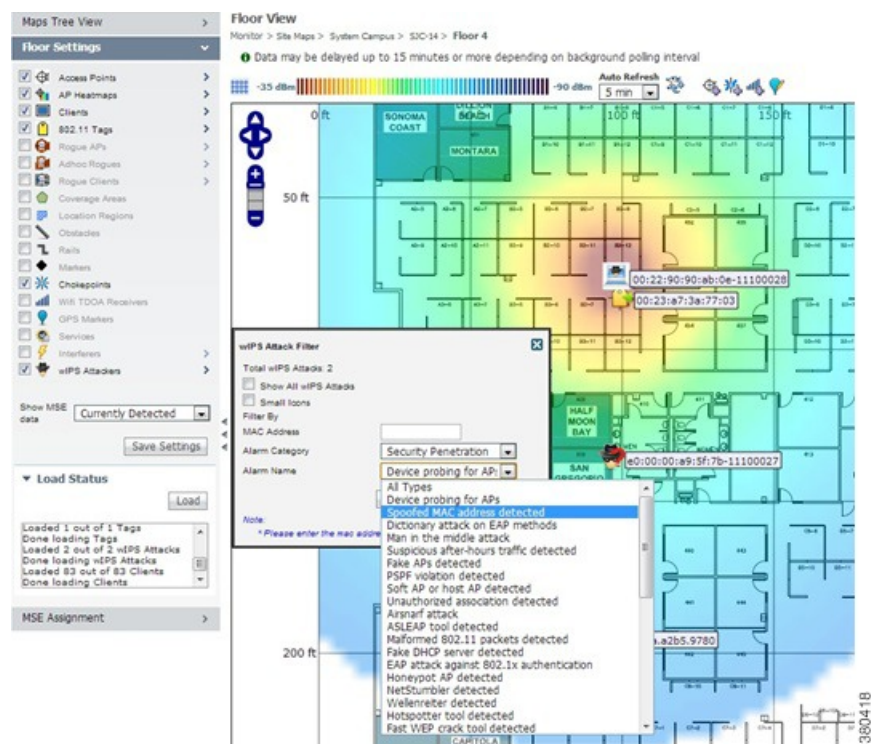


Note The alarm name is populated based on the alarm category selected.

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

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

Figure 2: wIPS Attack Name Filtering



The following icons are used to distinguish between devices displayed on the map.

Figure 3: Icons

Attacker:



Victim



Unknown Device



Import Map and AP Location Data

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



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



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

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

-
- Step 1** Choose Monitor > Site Maps.
- Step 2** From the Select a command drop-down list, choose Import Maps, and click Go.
- Step 3** Choose the WLSE Map and AP Location Data option, and click Next.
- Step 4** In the Import WLSE Map and AP Location Data page, click Browse to select the file to import.
- Step 5** Find and select the .tar file to import and click Open.
The Prime Infrastructure displays the name of the file in the Import From text box.
- Step 6** Click **Import**.
The CS uploads the file and temporarily saves it into a local directory while it is being processed. If the file contains data that cannot be processed, the Prime Infrastructure prompts you to correct the problem and retry. Once the file has been loaded, the Prime Infrastructure displays a report of what is added to the Prime Infrastructure. The report also specifies what cannot be added and why.
- If some of the data to be imported already exists, the Prime Infrastructure either uses the existing data in the case of campuses or overwrites the existing data using the imported data in the cases of buildings and floors.
- Note** If there are duplicate names between a WLSE site and building combination and an Prime Infrastructure campus (or top-level building) and building combination, the Prime Infrastructure displays a message in the Pre Execute Import Report indicating that it will delete the existing building.
- Step 7** Click Import to import the WLSE data.

The Prime Infrastructure displays a report indicating what was imported.

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

Monitoring the Floor Area

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

This section contains the following topics:

- [Planning and Zooming with Next Generation Maps](#), on page 146
- [Adding Access Points to a Floor Area](#), on page 147
- [Placing Access Points](#), on page 148

Planning and Zooming with Next Generation Maps

Planning

To move the map, click and hold the left mouse button and drag the map to a new place. You 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.



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

Zooming in and out - changing the scale

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

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



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

Adding Access Points to a Floor Area

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



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

- Step 1** Choose **Design > Site Maps**.
- Step 2** From the Maps Tree View or the Design > Site Maps left sidebar menu, choose the applicable floor to open the Floor View page.
- Step 3** From the Select a command drop-down list, choose **Add Access Points**, and click **Go**.
- Step 4** In the Add Access Points page, select the check boxes of the access points that you want to add to the floor area.
- Note** If you want to search for access points, enter AP name or MAC address (Ethernet/Radio)/IP in the Search AP [Name/Mac Address (Ethernet/Radio)/IP] text box, and then click **Search**. The search is case-insensitive.
- Note** Only access points that are not yet assigned to any floor or outdoor area appear in the list.
- Note** Select the check box at the top of the list to select all access points.
- Step 5** When all of the applicable access points are selected, click **OK** located at the bottom of the access point list. The Position Access Points page appears.
- Each access point you have chosen to add to the floor map is represented by a gray circle (differentiated by access point name or MAC address) and is lined up in the upper left part of the floor map.
- Step 6** Click and drag each access point to the appropriate location. Access points turn blue when selected.
- Note** When you drag an access point on the map, its horizontal and vertical position appears in the Horizontal and Vertical text boxes.
- Note** The small black arrow at the side of each access point represents Side A of each access point, and each access point arrow must correspond with the direction in which the access points were installed. Side A is clearly noted on each 1000 series access point and has no relevance to the 802.11a/n radio. To adjust the directional arrow, choose the appropriate orientation from the Antenna Angle drop-down list.
- When selected, the access point details are displayed on the left side of the page. Access point details include the following:
- AP Model—Indicates the model type of the selected access point.
 - Protocol—Choose the protocol for this access point from the drop-down list.
 - Antenna—Choose the appropriate antenna type for this access point from the drop-down list.
 - Antenna/AP Image—The antenna image reflects the antenna selected from the Antenna drop-down list. Click the arrow at the top right of the antenna image to expand the image size.
 - Antenna Orientation—Depending on the antenna type, enter the Azimuth and the Elevation orientations in degrees.
- Note** The Azimuth option does not appear for Omnidirectional antennas because their pattern is non directional in azimuth.

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

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

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

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

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

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

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

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

Note Note

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

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

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

Placing Access Points

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

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

- 1 Most importantly, access points should surround the desired location.
- 2 One access point should be placed roughly every 50 to 70 linear feet (about 17 to 20 meters). This translates into one access point every 2,500 to 5000 square feet (about 230 to 450 square meters).



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

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



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



Note If you have a ceiling-mounted AP with an integrated omni-directional antenna, the antenna orientation does not really need to be set in the Prime Infrastructure. However, if you mount that same AP on the wall, you must set the antenna orientation to 90 degrees. See [Placing Access Points, on page 148](#) for information on orientation of the access points.

Table 20: Antenna Orientation of the Access Points

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

Using the Automatic Hierarchy to Create Maps

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



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

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

-
- Step 1** Choose **Design > Automatic Hierarchy Creation** to display the Automatic Hierarchy Creation page.
- Step 2** In the text box, enter the name of an access point on your system. Or, you can choose one from the list. This name is used to create a regular expression to create your maps.
- Note** To update a previously created regular expression, select **Load and Continue** next to the expression and update the expression accordingly.
To delete a regular expression, select **Delete** next to the expression.
- Step 3** Click **Next**.
- Step 4** If your access point's name has a delimiter, enter it in the text box and click **Generate**. The system generates a regular expression that matches your access point's name based on the delimiter.
For example, using the dash (-) delimiter in the access point name San Jose-01-GroundFloor-AP3500i1, produces the regular expression `/(.*)-(.*)-(.*)-(.*)/`.
If you have a more complicated access point name, you can manually enter the regular expression.
- Note** You are not required to enter the leading and trailing slashes.
- Step 5** Click **Test**. The system displays the maps that will be created for the access point name and the regular expression entered.
- Step 6** Using the Group fields, assign matching groups to hierarchy types.
For example, if your access point is named: SJC14-4-AP-BREAK-ROOM
In this example, the campus name is SJC, the building name is 14, the floor name is 4, and the AP name is AP-BREAK-ROOM.
Use the regular expression: `/([A-Z]+)(\d+)-(\d+)-(.*)/`
From the AP name, the following groups are extracted:
- 1 SJC
 - 2 14
 - 3 4
 - 4 AP-BREAK-ROOM
- The matching groups are assigned from left to right, starting at 1. To make the matching groups match the hierarchy elements, use the drop-down list for each group number to select the appropriate hierarchy element.
This enables you to have almost any ordering of locations in your access point names.
For example, if your access point is named: EastLab-Atrium2-3-San Francisco
If you use the regular expression: `/(.*)-(.*)-(.*)-(.*)/` with the following group mapping:
- 1 Building
 - 2 Device Name
 - 3 Floor
 - 4 Campus

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

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

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

Table 21: Groups

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

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

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

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

Step 7

Click **Next**. You can test against more access points. You may test your regular expression and matching group mapping against more access points by entering the access point's names in the Add more device names to test against field, and clicking the **Add** button.

You then click the **Test** button to test each of the access points names in the table. The result of each test is displayed in the table.

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

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

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

Using the Map Editor

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

- [Guidelines for Using the Map Editor, on page 152](#)
- [Guidelines for Inclusion and Exclusion Areas on a Floor, on page 153](#)
- [Opening the Map Editor, on page 153](#)
- [Using the Map Editor to Draw Coverage Areas, on page 153](#)
- [Defining an Inclusion Region on a Floor, on page 154](#)
- [Defining an Exclusion Region on a Floor, on page 155](#)
- [Defining a Rail Line on a Floor, on page 155](#)

Guidelines for Using the Map Editor

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



Note

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

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

**Note**

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

- All walls are used by the Prime Infrastructure when generating RF coverage heatmaps.

Guidelines for Inclusion and Exclusion Areas on a Floor

Inclusion and exclusion areas can be of any polygon shape having at least three points.

You can only define one inclusion region on a floor. By default, an inclusion region is defined for each floor when it is added to the Prime Infrastructure. The inclusion region is indicated by a solid aqua color line, and generally outlines the region.

You can define multiple exclusion regions on a floor.

Newly defined inclusion and exclusion regions appear on heatmaps only after the Mobility Services Engine recalculates location on the floor.

Opening the Map Editor

To open the map editor, follow these steps:

-
- Step 1** Choose **Design > Site Map Design**.
 - Step 2** Click the desired campus. The Site Maps > Campus Name page appears.
 - Step 3** Click a campus and then click a building.
 - Step 4** Click the desired floor area. The Site Maps > Campus Name > Building Name > Floor Area Name page appears.
 - Step 5** From the Select a command drop-down list, choose **Map Editor**, and click **Go**. The Map Editor page appears.
-

Using the Map Editor to Draw Coverage Areas

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

To draw coverage areas using the map editor, follow these steps:

-
- Step 1** Add the floor plan if it is not already represented in the Prime Infrastructure.
 - Step 2** Choose **Monitor > Site Maps**.
 - Step 3** Click the Map Name that corresponds to the outdoor area, campus, building, or floor you want to edit.
 - Step 4** From the Select a command drop-down list, choose **Map Editor**, and click **Go**.
 - Step 5** 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.
-

Defining an Inclusion Region on a Floor

To define an inclusion area, follow these steps:

-
- Step 1** Choose **Design > Site Maps**.
- Step 2** Click the name of the appropriate floor area.
- Step 3** From the Select a command drop-down list, choose **Map Editor**.
- Step 4** Click **Go**.
- Step 5** At the map, click the aqua box on the toolbar.
- Note** A message box appears reminding you that only one inclusion area can be defined at a time. Defining a new inclusion region automatically removes the previously defined inclusion region. By default, an inclusion region is defined for each floor when it is added to the Prime Infrastructure. The inclusion region is indicated by a solid aqua line and generally outlines the region.
- Step 6** Click **OK** in the message box that appears. A drawing icon appears to outline the inclusion area.
- Step 7** To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.
- Step 8** Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.
- Step 9** Repeat [Defining an Inclusion Region on a Floor](#) until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area.
- Step 10** Choose **Save** from the Command menu or click the **disk** icon on the toolbar to save the inclusion region.
- Note** If you made an error in defining the inclusion area, click the area. The selected area is outlined by a dashed aqua line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.
- Step 11** Select the **Location Regions** check box if it is not already selected. If you want it to apply to all floor maps, click **Save settings**. Close the Layers configuration page.
- Step 12** To resynchronize the Prime Infrastructure and MSE databases, choose **Services > Synchronize Services**.
- Note** If the two databases are already synchronized then a resynchronization happens automatically every time there is a change. There is no need for an explicit resynch.
- Step 13** In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Note Newly defined inclusion and exclusion regions are included in location calculation only after the Mobility Services Engine recalculates location for existing devices.

Defining an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas exclusion areas in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are generally defined within the borders of an inclusion area.

To define an exclusion area, follow these steps:

-
- Step 1** Choose **Design > Site Maps**.
- Step 2** Click the name of the appropriate floor area.
- Step 3** From the Select a command drop-down list, choose **Map Editor**.
- Step 4** Click **Go**.
- Step 5** On the map, click the purple box on the toolbar.
- Step 6** Click **OK** in the message box that appears. A drawing icon appears to outline the exclusion area.
- Step 7** To begin defining the exclusion area, move the drawing icon to a starting point on the map and click once.
- Step 8** Move the drawing icon along the boundary of the area you want to exclude. Click once to start a boundary line, and click again to end the boundary line.
- Step 9** Repeat [Defining an Exclusion Region on a Floor](#) until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is completely defined. The excluded area is shaded in purple.
- Step 10** When all exclusion areas are defined, choose **Save** from the Command menu or click the **disk** icon on the toolbar to save the exclusion region.
- Note** To delete an exclusion area, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.
- Step 11** Select the **Location Regions** check box if it is not already selected. If you want it to apply to all floor maps, click **Save settings**. Close the Layers configuration page when complete.
- Step 12** To resynchronize the Prime Infrastructure and MSE databases, choose **Services > Synchronize 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.
-

Defining a Rail Line on a Floor

You can define a rail line on a floor that represents a conveyor belt. Additionally, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area

in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority).



Note Rail line configurations do not apply to tags.

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

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

-
- Step 1** Choose **Design > Site Maps**.
 - Step 2** Click the name of the appropriate floor area.
 - Step 3** Choose **Map Editor** from the Select a command drop-down list.
 - Step 4** Click **Go**.
 - Step 5** In the map, click the **rail** icon (to the right of the purple exclusion icon) on the toolbar.
 - Step 6** In the message dialog box that appears, enter a snap-width (feet or meters) for the rail and then click **OK**. A drawing icon appears.
 - Step 7** Click the **drawing** icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.
 - Step 8** Click the **drawing** icon twice when the rail line is completely drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.
 - Note** To delete a rail line, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.
 - Step 9** At the floor map, choose the **Layers** drop-down list.
 - Step 10** Select the **Rails** check box for if it is not already selected, click **Save settings**, and close the Layers configuration panel when complete.
 - Step 11** To resynchronize the Prime Infrastructure and Mobility Services Engine, choose **Services > Synchronize Services**.
 - Step 12** In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**. You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.
-

Adding an Outdoor Area



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

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

-
- Step 1** If you want to add a map of the outdoor area to the database, save the map in .PNG, .JPG, .JPEG, or .GIF format. Then browse to and import the map from anywhere in your file system.
- Note** You do not need a map to add an outdoor area. You can simply define the dimensions of the area to add it to the database. The map can be any size because the Prime Infrastructure automatically resizes the map to fit the workspace.
- Step 2** Choose **Design > Site Maps**.
- Step 3** Click the desired campus to display the Design > Site Maps > Campus View page.
- Step 4** From the Select a command drop-down list, choose **New Outdoor Area**.
- Step 5** Click **Go**. The Create New Area page appears.
- Step 6** In the New Outdoor Area page, enter the following information:
- Name—The user-defined name of the new outdoor area.
 - Contact—The user-defined contact name.
 - Area Type (RF Model)—Cubes And Walled Offices, Drywall Office Only, Outdoor Open Space (default).
 - AP Height (feet)—Enter the height of the access point
 - Image File—Name of the file containing the outdoor area map. Click **Browse** to find the file.
- Step 7** Click **Next**.
- Step 8** Click **Place** to put the outdoor area on the campus map. the Prime Infrastructure creates an outdoor area rectangle scaled to the size of the campus map.
- Step 9** Click and drag the outdoor area rectangle to the desired position on the campus map.
- Step 10** Click **Save** to save this outdoor area and its campus location to the database.
- Note** A hyperlink associated with the outdoor area takes you to the corresponding Maps page.
- Step 11** (Optional) To assign location presence information for the new outdoor area, choose **Edit Location Presence Info**, and click **Go**.
- Note** By default, the Override Child Element Presence Info check box is selected. There is no need to alter this setting for outdoor areas.
-

Using Planning Mode

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

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

**Note**

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

Planning Mode options:

- Add APs—Enables you to add access points on a map. See the “Adding Access Points to a Floor Area” section on page 10-11 for details.
- Delete APs—Deletes the selected access points.
- Map Editor—Opens the Map Editor window.
- Synchronize with Deployment—Synchronizes your planning mode access points with the current deployment scenario.
- Generate Proposal—View a planning summary of the current access points deployment.
- Planned AP Association Tool—Allows you to add, delete, or import an AP Association from an Excel or CSV file. Once an access point is defined, it can be associated to a base radio MAC address using the Planned AP Association Tool. If the AP is not discovered, then the APs gets pushed into a standby bucket and get associated when discovered.

**Note**

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

**Note**

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

Using Chokepoints to Enhance Tag Location Reporting

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be entered into the location database and plotted on the Prime Infrastructure map.

Using chokepoints in conjunction with active Cisco CX compliant tags provides immediate location information on a tag and its asset. When a Cisco CX tag moves out of the range of a chokepoint, its subsequent beacon frames do not contain any identifying chokepoint information. Location determination of the tag defaults to the standard calculation methods based on RSSIs reported by access points associated with the tag.

- [Adding Chokepoints to the Prime Infrastructure, on page 159](#)
- [Adding a Chokepoint to a Prime Infrastructure Map, on page 159](#)
- [Removing Chokepoints from the Prime Infrastructure, on page 160](#)

Adding Chokepoints to the Prime Infrastructure

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

-
- Step 1** Choose **Configure > Chokepoints**.
- Step 2** From the Select a command drop-down list, choose **Add Chokepoints**.
- Step 3** Click **Go**.
- Step 4** Enter the MAC address and name for the chokepoint.
- Step 5** Select the **Entry/Exit Chokepoint** check box.
- Step 6** Enter the coverage range for the chokepoint.
Note The Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.
- Step 7** Click **OK**.
Note After the chokepoint is added to the database, it can be placed on the appropriate the Prime Infrastructure floor map.
-

Adding a Chokepoint to a Prime Infrastructure Map

To add the chokepoint to a map, follow these steps:

-
- Step 1** Choose **Design > Site Maps**.
- Step 2** In the Maps page, choose the link that corresponds to the floor location of the chokepoint.
- Step 3** From the Select a command drop-down list, choose **Add Chokepoints**.
- Step 4** Click **Go**.
Note The Add Chokepoints summary page lists all recently added chokepoints that are in the database but are not yet mapped.
- Step 5** Select the check box next to the chokepoint that you want to place on the map.
- Step 6** Click **OK**.
A map appears with a chokepoint icon located in the top left-hand corner. You are now ready to place the chokepoint on the map.
- Step 7** Left-click the chokepoint icon and drag it to the proper location.
Note The MAC address, name, and coverage range of the chokepoint appear in the dialog box in the left when you click the chokepoint icon for placement.
- Step 8** Click **Save**.
The floor map page reappears and the added chokepoint appears on the map.
Note The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.

Note The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

Note The MAC address, name, entry or exit chokepoint, static IP address, and range of the chokepoint appear when you hover your mouse cursor over its map icon.

Step 9 If the chokepoint does not appear on the map, select the **Chokepoints** check box located in the Floor Settings menu.

Note Do not click **Save Settings** unless you want to save this display criteria for all maps.

Note You must synchronize network design to the Mobility Services Engine or location server to push chokepoint information.

Removing Chokepoints from the Prime Infrastructure

You can remove one or more chokepoints at a time. To delete a chokepoint, follow these steps:

Step 1 Choose **Configure > Chokepoints**. The Chokepoints page appears.

Step 2 Select the check box next to the chokepoint to be deleted.

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

Step 4 To confirm the chokepoint deletion, click **OK** in the dialog box that appears. The Chokepoints page reappears and confirms the deletion of the chokepoints. The deleted chokepoints are no longer listed in the page.



Monitoring the System and Services

This chapter describes how to monitor the Cisco Mobility Services Engine by configuring and viewing alarms, events, and logs and how to generate reports on system use and element counts (tags, clients, rogue clients, interferers, and access points). This chapter also describes how to use the Prime Infrastructure to monitor clients (wired and wireless), tags, chokepoints, and Wi-Fi TDOA receivers.

- [Working with Alarms, page 162](#)
- [Working with Events, page 166](#)
- [Working with Logs, page 167](#)
- [Generating Reports, page 169](#)
- [Generating MSE Analytics Reports, page 178](#)
- [Creating a Device Utilization Report, page 195](#)
- [Managing OUI, page 197](#)
- [Monitoring Wireless Clients, page 198](#)
- [Client Support on the MSE, page 202](#)
- [Configuring Buildings, page 209](#)
- [Monitoring Tags, page 213](#)
- [Monitoring Geo-Location, page 217](#)
- [Monitoring Chokepoints, page 218](#)
- [Monitoring Wi-Fi TDOA Receivers, page 219](#)
- [Ekahau Site Survey Integration, page 220](#)
- [AirMagnet Survey and Planner Integration, page 221](#)
- [Monitoring Wired Clients, page 221](#)
- [Monitoring Wired Switches, page 222](#)
- [Monitoring Interferers, page 223](#)
- [Clustering of Monitor Mode APs Using MSE, page 225](#)

Working with Alarms

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

- [Guidelines and Limitations](#), on page 162
- [Viewing Alarms](#), on page 162
- [Monitoring Cisco Adaptive wIPS Alarm Details](#), on page 163
- [Assigning and Unassigning Alarms](#), on page 165
- [Deleting and Clearing Alarms](#), on page 165
- [E-mailing Alarm Notifications](#), on page 165

Guidelines and Limitations

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

Viewing Alarms

To view Mobility Services Engine alarms, follow these steps:

-
- Step 1** Choose **Monitor > Alarms**.
- Step 2** Click the **Advanced Search** link in the navigation bar. A configurable search dialog box for alarms appears.
- Step 3** Choose **Alarms** from the Search Category drop-down list.
- Step 4** Choose the severity of alarms from the Severity drop-down list. The options are All Severities, Critical, Major, Minor, Warning, or Clear.
- Step 5** Choose **Mobility Service** from the Alarm Category drop-down list.
- Step 6** Choose the **Condition** from the Condition combo box. Alternatively, you can enter the condition in the Condition text box.
- Step 7** From the Time Period drop-down list, choose the time frame for which you want to review alarms. The options range from minutes (5, 15, and 30) to hours (1 and 8) to days (1 and 7). To display all, choose **Any time**.
- Step 8** Select the **Acknowledged State** check box to exclude the acknowledged alarms and their count in the Alarm Summary page.
- Step 9** Select the **Assigned 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](#).

Monitoring Cisco Adaptive wIPS Alarm Details

To view MSE alarm details, follow these steps:

Choose **Monitor** > **Alarms** > *failure object* to view details of the selected Cisco wIPS alarm. The following alarm details are provided for Cisco Adaptive wIPS alarms:

- **General Properties**—The general information might vary depending on the type of alarm. For example, some alarm details might include location and switch port tracing information. The following table describes the general parameters associated with the MSE Alarm and wIPS Traps condition.
 - **Detected By wIPS AP**—The access point that detected the alarm.
 - **wIPS AP IP Address**—The IP address of the wIPS access point.
 - **Owner**—Name of person to which this alarm is assigned or left blank.
 - **Acknowledged**—Displays whether or not the alarm is acknowledged by the user.
 - **Category**—For wIPS, the alarm category is Security.
 - **Created**—Month, day, year, hour, minute, second, AM or PM that the alarm was created.
 - **Modified**—Month, day, year, hour, minute, second, AM or PM that the alarm was last modified.
 - **Generated By**—Indicates how the alarm event was generated (either NMS or from a trap).
 - NMS (Network Management System - Prime Infrastructure)—Generated through polling. Prime Infrastructure periodically polls the Cisco WLCs and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events. In this case, "Generated by" NMS.
 - Trap—Generated by the controller. Prime Infrastructure processes these traps and raises corresponding events for them. In this case, "Generated by" is controller.
 - **Severity**—Level of severity including critical, major, minor, warning, and clear.
 - **Last Disappeared**—The date and time that the potential attack last disappeared.
 - **Channel**—The channel on which the potential attack occurred.
 - **Attacker Client/AP MAC**—The MAC address of the client or access point that initiated the attack.
 - **Attacker Client/AP IP Address**—The IP address of the client or access point that initiated the attack.

- Target Client/AP IP Address—The IP address of the client or access point targeted by the attacker.
 - Controller IP Address—The IP address of the controller to which the access point is associated.
 - MSE—The IP address of the associated Mobility Services Engine.
 - Controller MAC address—The MAC address of the controller to which the access point is associated.
 - wIPS access point MAC address
 - Forensic File
 - Event History—Takes you to the Monitoring Alarms page to view all events for this alarm.
- Annotations—Enter any new notes in this text box and click **Add** to update the alarm. Notes appear in the "Annotations" display area.
 - Messages—Displays the alarm name.
 - Description—Displays the consolidated information about the alarm.
 - Mitigation Status—Displays what mitigation action was initiated against the attack.
 - Audit Report—Click to view config audit alarm details. This report is only available for Config Audit alarms.

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



Note If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group. The alarms have links to the audit report where you can view a list of discrepancies for each controller.

- Event History—Opens the MSE Alarm Events page to view events for this alarm. When there are multiple alarm pages, the page numbers appear at the top of the page with a scroll arrow on each side. Use these scroll arrows to view additional alarms.
- Rogue Clients—If the failure object is a rogue access point, information about rogue clients is displayed.
- Map Location—Displays the map location for the alarm.
 - Floor—The location where this attack was detected.
 - Last Located At—The last time where the attack was located.
 - On MSE—The mobility server engine in which this attack was located.
 - Location History—Click the Location History to see details on the current attacker and victim location.
- Related Alarm List—Lists all the alarms related to a particular attack. This shows what consolidation rule was used to consolidate the alarms.
 - Alarm Name—Name of the alarm.
 - First Heard—Indicates the date and time when the attack first seen.
 - Last Heard—Indicates the date and time when the attack was last seen.

◦ Status—Status of the attack.

Assigning and Unassigning Alarms

To assign and unassign an alarms, follow these steps:

-
- Step 1** Choose **Monitors > Alarms** to display the Alarms page.
- Step 2** Select the alarms that you want to assign to yourself by selecting their corresponding check boxes.
- Note** To unassign an alarm assigned to you, unselect the box next to the appropriate alarm. You cannot unassign alarms assigned to others.
- Step 3** Choose **Assign > Assign to Me (or Unassign)**. From the Select a command drop-down list, choose Assign to Me (or Unassign). Click **Go**.
- If you choose Assign to Me, your username appears in the Owner column. If you choose Unassign, the username column becomes empty.
-

Deleting and Clearing Alarms

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

To delete or clear an alarm from a Mobility Services Engine, follow these steps:

-
- Step 1** Choose **Monitors > Alarms** to display the Alarms page.
- Step 2** Select the alarms that you want to delete or clear by selecting their corresponding check boxes.
- Step 3** From the Select a command drop-down list, choose **Delete** or **Clear**. Click **Go**.
-

E-mailing Alarm Notifications

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

You can choose the alarm severity types (critical, major, minor, and warning) to have e-mailed to you.

To send alarm notifications to e-mail, follow these steps:

-
- Step 1** Choose **Monitor > Alarms**.
- Step 2** Select the alarms by selecting their corresponding check boxes. Click **Email Notification**. 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 **OKSave**.
You are returned to the Alarms > Notification page. The changes to the reported alarm severity levels and the recipient e-mail address for e-mail notifications are displayed.
-

Working with Events

You can use Prime Infrastructure to view the Mobility Services Engine and location notification events. You can search and display events based on their severity (critical, major, minor, warning, clear, and info) and their category.

This section contains [Displaying Location Notification Events](#) procedure.

Displaying Location Notification Events

To display location notification events, follow these steps:

-
- Step 1** Choose **Monitor > Events**.
- Step 2** In the Events page, you can perform the following:
- If you want to display the events for a specific element, and you know its IP address, name, WLAN SSID, or MAC address, enter that value in the Search text box of the navigation bar. Click **Search**.
 - To display events by severity and category, click **Advanced Search** in the navigation bar and choose the appropriate options from the Severity and Event Category drop-down lists box. Click **Go**.
- Step 3** If Prime Infrastructure finds events that match the search criteria, it shows a list of these events.

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

Working with Logs

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

- [Guidelines and Limitations](#), on page 167
- [Configuring Logging Options](#), on page 167
- [MAC address-based Logging](#), on page 168
- [Downloading Log Files](#), on page 168

Guidelines and Limitations

- When you are selecting an appropriate option from the logging level, make sure you use Error and Trace only when directed to do so by Cisco TAC personnel.
- Enable advanced debugging only under the guidance of Cisco TAC personnel because advanced debugging slows the mobility service down.

Configuring Logging Options

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

To configure logging options, follow these steps:

-
- Step 1** Choose **Services > Mobility Services****Mobility Services Engines**.
- Step 2** Click the name of the MSE that you want to configure.
- Step 3** From the System menu, choose **Logs**. The logging options for the selected MSE appear.
- Step 4** Choose the appropriate options from the Logging Level drop-down list.
There are four logging options: **Off**, **Error**, **Information**, and **Trace**.
- All log records with a log level of **Error** or above are logged to a new error log file `locserver-error-%u-%g.log`. This is an additional log file maintained along with the location server `locserver-%u-%g.log` log file. The error log file consists of logs of **Error** level along with their context information. The contextual information consists of 25 log records prior to the error. You can maintain up to 10 error log files. The maximum size allowed for each log file is 10 MB.
- Caution** Use **Error** and **Trace** only when directed to do so by Cisco Technical Assistance Center (TAC) personnel.
- Step 5** Select the **Enable** check box next to each element listed in that section to begin logging of its events.
- Step 6** Select the **Enable** check box under Advanced Parameters to enable advanced debugging. By default, this option is disabled.

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

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

Step 8 In the Log File group box, enter the following:

- The number of log files to be maintained in the MSE. You can maintain a minimum of 5 log files and a maximum of 20 log files in the MSE.
- The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.

Step 9 In the MAC Address Based Logging page, do the following:

- Select the **Enable** check box to enable MAC address logging. By default, this option is disabled.
- Add one or more MAC addresses for which you want to enable logging. You can also remove MAC addresses that you have already added by selecting the MAC address from the list and clicking **Remove**.

For more information on MAC-address-based logging, see the [MAC address-based Logging](#).

Step 10 Click **Save** to apply your changes.

MAC address-based Logging

This feature allows you to create log files that are specific to an entity whose MAC address is specified. The log files are created in the locserver directory under the following path:

```
/opt/mse/logs/locserver
```

A maximum of 5 MAC addresses can be logged at a time. The log file format for MAC address aa:bb:cc:dd:ee:ff is:

```
macaddress-debug-aa-bb-cc-dd-ee-ff.log
```

You can create a maximum of two log files for a MAC address. The two log files may consist of one main and one back up or rollover log file.

The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC address. The MAC log files which are not updated for more than 24 hours are pruned.

Downloading Log Files

If you need to analyze Mobility Services Engine log files, you can use Prime Infrastructure to download them to your system. The Prime Infrastructure downloads a .zip file containing the log files.

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

-
- Step 1** Choose **Services > Mobility Services**.
- Step 2** Click the name of the Mobility Services Engine to view its status.
- Step 3** From the left sidebar menu, choose **Logs**.
- Step 4** Click **Download Logs**.
- Step 5** Follow the instructions in the File Download dialog box to view the file or save the .zip file to your system.
-

Generating Reports

In the Prime Infrastructure, you can generate various kinds of reports. This section explains how to generate Context Aware reports using the Prime Infrastructure Report Launch Pad. By default, reports are stored on the Prime Infrastructure server.

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

You can define the following criteria for the reports:

- Which Mobility Services Engine or engines to monitor
- How often the report is generated
- How the data is graphed on the charts
- Whether the report is e-mailed or exported to a file

Report Launch Pad

The report launch pad provides access to all the Prime Infrastructure reports from a single page. In this page, you can view current reports, open specific types of reports, create and save new reports, and manage scheduled runs. You can access the ContextAware reports section in the Report Launch Pad to generate ContextAware reports.

**Tip**

Hover your mouse cursor over the tool tip next to the report type to view more report details.

- [Creating and Running a New Report](#), on page 170
- [Managing Current Reports](#), on page 175
- [Managing Scheduled Run Results](#), on page 175
- [Managing Saved Reports](#), on page 176

Creating and Running a New Report

To create and run a new report, follow these steps:

-
- Step 1** Choose **Reports > Report Launch Pad**.
The reports are listed by category in the main section of the page and on the left sidebar menu.
- Step 2** Find the appropriate report in the main section of the Report Launch Pad.
Note Click the report name from the Report Launch Pad or use the navigation on the left side of the Report Launch Pad page to view any currently saved reports for that report type.
- Step 3** Click **New**. The Report Details page appears.
- Step 4** In the Report Details page, enter the following Settings parameters:
Note Certain parameters may or may not appear depending on the report type.
- Report Title—If you plan to use this as a saved report, enter a report name.
 - Report By—Choose the appropriate Report By category from the drop-down list.
 - Report Criteria—Allows you to sort your results depending on the previous Report By selection made. Click Edit to open the Filter Criteria page.
Note Click **Select to confirm your filter criteria** or Close to return to the previous page.
 - Connection Protocol—All Clients, All Wired(802.3), All Wireless (802.11), All 11u Capable Clients, 802.11a/n, 802.11b/g/n, 802.11a, 802.11b, 802.11g, 802.11n (5 GHz), 802.11n (2.4 GHz).
 - Reporting Period
 - Select the reporting period from the Select a time period...drop-down list. The possible values are Today, Last 1 Hour, Last 6 Hours, Last 12 hours, Last 1 Day, Last 2 Days, Last 3 days, Last 4 Days, Last 5 Days, last 6 Days, Last 7 Days, Last 2 Weeks, Last 4 weeks, Previous Calendar Month, Last 8 Weeks, Last 12 Weeks, Last 6 Months, and Last 1 Year.
 - From—Select the From radio button and enter the From and To dates and times. You can type a date in the text box, or click the Calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.
 - Show—Enter the number of records that you want to be displayed on each page.
Note Leave the text box blank to display all records.
- Step 5** If you plan to run this report at a later time or as a recurring report, enter the Schedule parameters. The Schedule parameters allow you to control when and how often the report runs.
- Scheduling—Select the Enable check box to run the report on the set schedule.
 - Export Format—Choose your format for exported files (CSV or PDF).
 - Destination—Select your destination type (File or E-mail). Enter the applicable file location or the e-mail address.

Note The default file locations for CSV and PDF files are as follows:

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

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

Note To set the mail server setup for e-mails, choose Administration > Settings, then choose Mail Server from the left sidebar menu to view the Mail Server Configuration page. Enter the SMTP and other required information.

- **Start Date/Time**—Enter a date in the provided text box, or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists. The report begins to run on this data and at this time.
- **Recurrence**—Enter the frequency of this report.
 - **No Recurrence**—The report runs only once (at the time indicated for the Start Date/Time).
 - **Hourly**—The report runs on the interval indicated by the number of hours you enter in the Entry text box.
 - **Daily**—The report runs on the interval indicated by the number of days you enter in the Every text box.
 - **Weekly**—The report runs on the interval indicated by the number of weeks you enter in the Every text box and on the days specified by the selected check boxes.
 - **Monthly**—The report runs on the interval indicated by the number of months you enter in the Every text box.

The Create Custom Report page allows you to customize the report results.

For the more information on the customizable reports, see *Cisco Prime Infrastructure User Guide*.

The following table specifies which reports are customizable, which have multiple sub-reports, and which report views are available. In future releases, all reports are customizable.

Table 22: 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
Client Count	Yes	No	Graphical	No
Client Session	Yes	No	Tabular	No
Client Summary	Yes	Yes	Various	Yes
Client Traffic	Yes	No	Graphical	No

Report	Customizable?	Multiple Sub-Reports?	Report Views	Data Field Sorting?
Client Traffic Stream Metrics	Yes	No	Tabular	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	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

Report	Customizable?	Multiple Sub-Reports?	Report Views	Data Field Sorting?
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
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

Report	Customizable?	Multiple Sub-Reports?	Report Views	Data Field Sorting?
wIPS Alarm	Yes	No	Tabular	No
wIPS Alarm Summary	Yes	No	Both	No
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

Step 6 Click **Customize** to open a separate Create Custom Report page.

- 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.
- 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.
- 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.

- 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.
- In the Data field sorting group box, indicate your sorting preference (Ascending or Descending). Determine how the report data is sorted.
 - You can select four data fields for which you can specify sorting order. Use the Sort by and Then by drop-down lists to select each data field for sorting.
 - For each sorted data field, select whether you want it sorted in Ascending or Descending order.

Note Only reports in table form (rather than graphs or combined) can be sorted. Only fields that can be sorted appear in the Data field sorting drop-down lists.

- f) Click **Apply** to confirm the changes, **Reset** to return columns to the default, or **Cancel** to close this page with no changes made.

Note The changes made in the Create Custom Report page are not saved until you click Save in the Report Details page.

Step 7 When all report parameters have been set, choose one of the following:

- **Save**—Click **Save** to save this report setup without immediately running the report. The report automatically runs at the scheduled time.
 - **Save and Run**—Click **Save and Run** to save this report setup and to immediately run the report.
 - **Run Now**—Click **Run Now** to run the report without saving the report setup.
 - **Cancel**—Click **Cancel** to return to the previous page without running nor saving this report.
-

Managing Current Reports

If a report has been saved for a specific report type, you can access the current reports from the Report Launch Pad.

When a new chokepoint is created, it is available in all the virtual domains. After placing it on a floor, it is updated so that it is available in the same virtual domain as that of a floor. When a chokepoint is removed from a floor, it will be available in all the virtual domains again.

To access current or saved reports from the Report Launch Pad, follow these steps:

Step 1 Choose **Reports > Report Launch Pad**

Step 2 Choose the specific report from the left sidebar menu or from the main section of the Report Launch Pad. The Report Launch Pad page displays a list of current reports for this report type. To view a list of saved reports, choose **Reports > Saved Reports**.

Managing Scheduled Run Results



Note The list of scheduled runs can be sorted by report category, report type, and time frame.

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. 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.

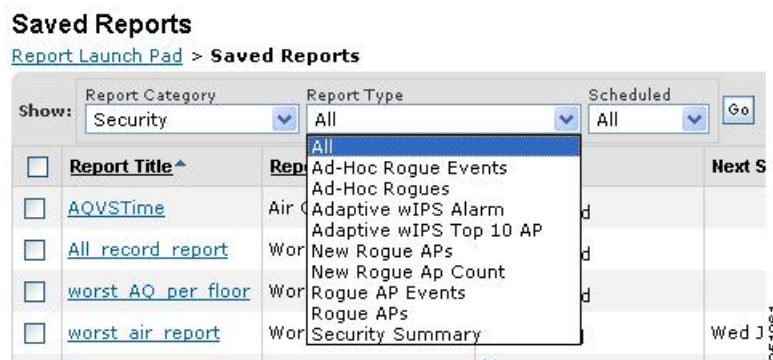
- Download—Click the Download icon to open or save a .csv file of the report results.
- Run Now—Click the Run Now icon to immediately run the current report.

Sorting Saved Reports

You can use the Show drop-down lists to sort the Saved Reports list by category, type, and scheduled status.

- 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 4: Sorting Saved Reports



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 an MSE analytics report, click **New** next to a type.

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

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

- [Associated vs. Probing Clients by Selected Zone](#), on page 178
- [Client Location](#), on page 178
- [Client Location Density](#), on page 180
- [Device Count by Zone](#), on page 182
- [Device Dwell Time by Zone](#), on page 184
- [Guest Location Density](#), on page 185
- [Location Notifications by Zone](#), on page 187
- [Mobile MAC Statistics](#), on page 188
- [Rogue AP Location Density](#), on page 190
- [Rogue Client Location Density](#), on page 191
- [Tag Location Tracking](#), on page 193

Associated vs. Probing Clients by Selected Zone

This report provides counts for associated vs. probing clients in the selected time period on a selected zone. The first part of the report shows the count in a time series chart and the other part shows the distribution of the clients on the floor.

This section contains the following topics:

- [Configuring a associated vs. probing clients by selected zone report](#)
- [Associated vs. Probing client report results](#)

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 the non-root virtual domain.

This section contains the following topics:

- [Configuring a Client Location History Report, on page 179](#)
- [Client Location Results, on page 180](#)

Configuring a Client Location History 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 click **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, on page 176](#) 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, on page 176](#) 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 Cisco WLCs—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 the hyperlink shows the location of the client in the floor map at the located time. If the previous and current client location calculation is greater than 20 feet which is a configurable parameter, then the location history report is updated. This calculation is done every 30 to 120 seconds depending on the client.

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, on page 180](#)
- [Client Location Density Results, on page 182](#)

Configuring a Client Location Density 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
 - MSE By Floor Area
 - MSE By Outdoor Area
 - MSE
- Report Criteria—The report criteria differ 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 click **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.

Reporting Period

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



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

Schedule

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

Customize Report Form

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

**Note**

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

Client Location 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 the client.
- User—The username of the client.
- Detecting Cisco WLCs—The IP address of the detecting controller.
- 802.11 State—The state of 802.11. It can be 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 sections contains the following topics:

- [Configuring a Device Dwell by Zone Report, on page 182](#)
- [Device Count by Zone Results, on page 183](#)

Configuring a Device Dwell by Zone Report

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

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 differ 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 click **Close** to return to the previous page.

- Device Type
 - All
 - Clinet
 - 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. Choose the hours and minutes from the drop-down lists.



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

Schedule

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

Customize Report Form

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



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

Device Count by Zone Results

The results of the Device Count by Zone report contain 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.

- [Configuring a Device Dwell Time by Zone Report](#)
- [Device Count by Zone Results](#), on page 183

Configuring a Device Dwell by Zone Report

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

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 differ 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 click **Close** to return to the previous page.

- Device Type
 - All
 - Clinet
 - 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. Choose the hours and minutes from the drop-down lists.



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

Schedule

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

Customize Report Form

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



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

Device Count by Zone Results

The results of the Device Count by Zone report contain 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.

- [Configuring Guest Location Density, on page 185](#)
- [Guest Location Density Results, on page 186](#)

Configuring Guest Location Density

This section 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 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. 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, on page 176](#) for more information.

- **Customize Report Form**

The Customize Report form allows you to customize the report results. See the [Managing Saved Reports, on page 176](#) for more information on scheduling a report.

Guest Location Density Results

The results of the Guest Location Tracking report contains 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.

- 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 section contains the following topics:

- [Configuring a Location Notification Report, on page 187](#)
- [Location Notification Results, on page 188](#)

Configuring a Location Notification Report

This section describes how to configure a Rogue Client Location Tracking report.

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 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, on page 176](#) 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, on page 176](#) 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 Location Notification report contains 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 statistics based on click count by MSAP servers or by venues.

- [Configuring Mobile MAC Statistics, on page 188](#)
- [Mobile MAC Tracking Results, on page 189](#)

Configuring Mobile MAC Statistics

This section describes how to configure a Mobile MAC Statistics 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, on page 176](#) 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, on page 176](#) for more information on customizing report results.



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

Mobile MAC Tracking Results

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 Density, on page 190](#)

Configuring Rogue AP Location Density

This section describes how to configure a rogue AP location density 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
- 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
 - Clinet
 - 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. 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, on page 176](#) 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, on page 176](#) 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 Density

This report shows rogue client location density detected by the MSEs based on your filtering criteria.

- [Configuring Rogue Client Location Density, on page 191](#)
- [Rogue Client Location Tracking Results, on page 192](#)

Configuring Rogue Client Location Density

This section describes how to configure a Rogue Client Location Density 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. 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.

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, on page 176](#) 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, on page 176](#) 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 Rogue Client Location Tracking report contains 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—Position of the rogue client at the located time.
- MSE—Name of the MSE that located this rogue client.
- Rogue AP—The rogue access point to which the rogue client is associated with.
- Detecting Cisco WLCs—The IP address of the detecting controller.
- State—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 Tracking

This report shows the location tracking of a tag detected by an MSE.

This section contains the following topics:

- [Configuring Tag Location Tracking, on page 193](#)
- [Tag Location Tracking Results, on page 194](#)

Configuring 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 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, on page 176](#) 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, on page 176](#) 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 from these protocols: **All Clients**, **All Wired (802.3)**, **All Wireless (802.11)**, **802.11a/n**, **802.11b/g/n**, **802.11a**, **802.11b**, **802.11g**, **802.11n (5-GHz)**, or **802.11n (2.4-GHz)**.
- SSID—All SSIDs is the default value.
- Reporting Period—You can define the report to collect data hourly, weekly, or at a specific date and time. The selected reporting period type is displayed on the x-axis.

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

Step 5 In the Schedule group box, select the **Enable Schedule** check box.

Step 6 Choose the report format (CSV or PDF) from the Export Report drop-down list.

Step 7 Select either **File** or **Email** as the destination of the report.

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

Step 8 Enter a start date (MM:DD:YYYY), or click the **Calendar** icon to select a date.

Step 9 Specify a start time using the hour and minute drop-down lists.

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

- No Recurrence
- Hourly
- Daily
- Weekly

- Monthly

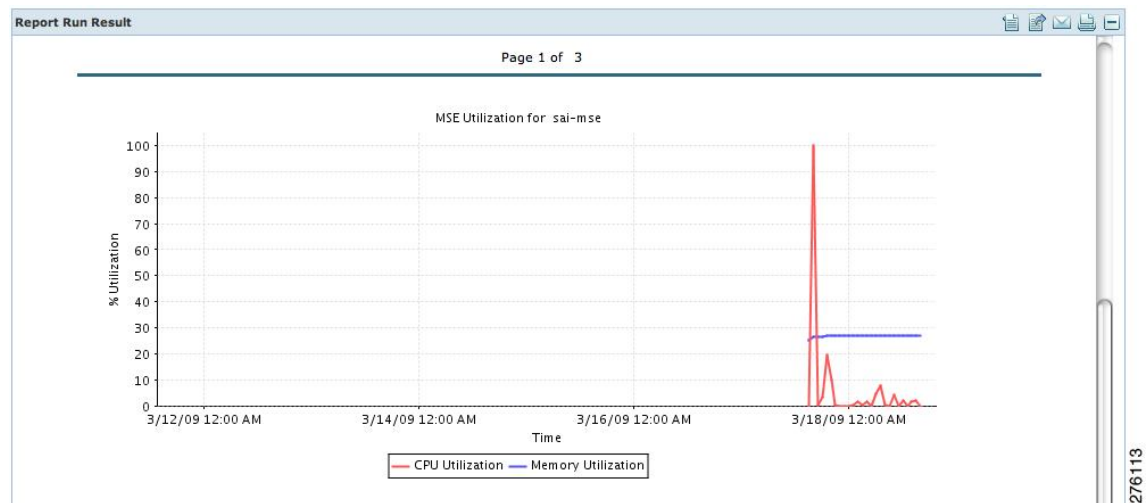
Note The days of the week appear on the page only when the weekly option is chosen.

Step 11 When finished with [Step 1](#) to [Creating a Device Utilization Report](#), do one of the following:

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

Note You can also click **Run Now** to check the defined report criteria before saving it or to run reports as necessary. Only the CPU and memory utilization reports are shown in the following example.

Figure 5: Devise > MSE Utilization > Results



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

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

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

Step 12 To enable, disable, or delete a report, select the check box next to the report title, and click the appropriate option.

Viewing Saved Utilization Reports

To download a saved report, follow these steps:

-
- Step 1** Choose **Reports > Saved Reports**.
- Step 2** Click the **Download** icon for your report. It is downloaded and saved in the defined directory or e-mailed.
-

Viewing Scheduled Utilization Runs

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

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

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. 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.
- [Adding a New Vendor OUI Mapping, on page 197](#)
- [Uploading an Updated Vendor OUI Mapping File, on page 198](#)

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**.
- Step 9** After adding new OUIs, you must restart the Prime Infrastructure server to make changes into effect. You can use the following commands to shut down and restart the Prime Infrastructure server.
- Stop the services using the **ncs stop** command.
 - Restart the services using the **ncs start** command.
-

Uploading an Updated Vendor OUI Mapping File

You can download and save the vendorMacs.xml file posted on cisco.com 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](#), on page 199
- [Monitoring Wireless Clients Using Search](#), on page 201

Monitoring Wireless Clients Using Maps

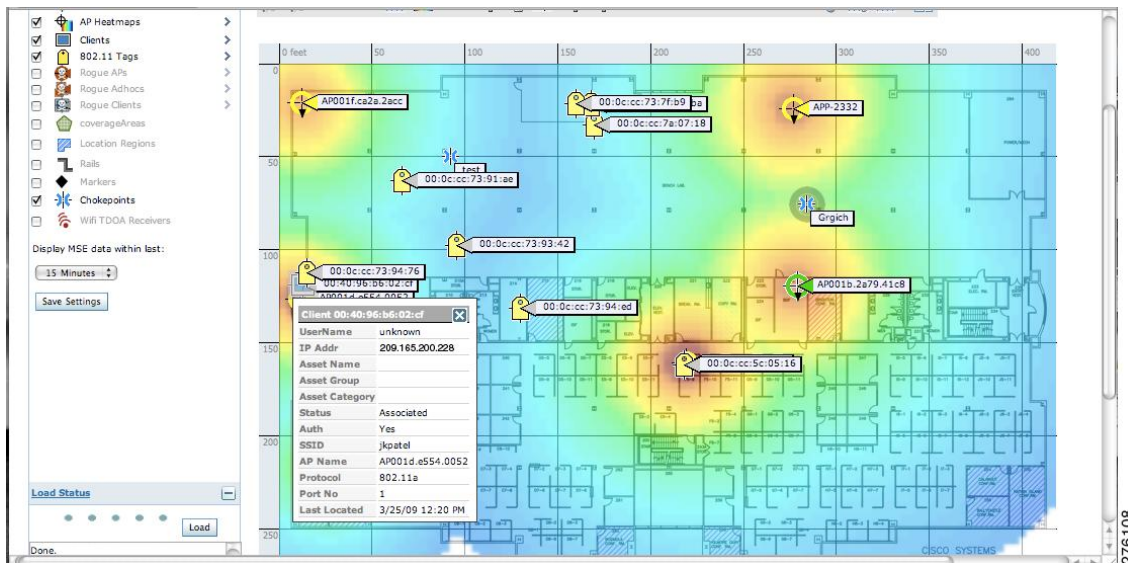
On a Prime Infrastructure map, you can view the name of the access point that the client is associated with, the IP Address, Asset information, Authentication, SSID, 802.11 protocol, and when the location information was last updated for the client. Hover mouse cursor over the client icon on the map 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. Do not click **Save Settings** unless you want to save changes made to the floor settings across all maps.

Figure 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 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.

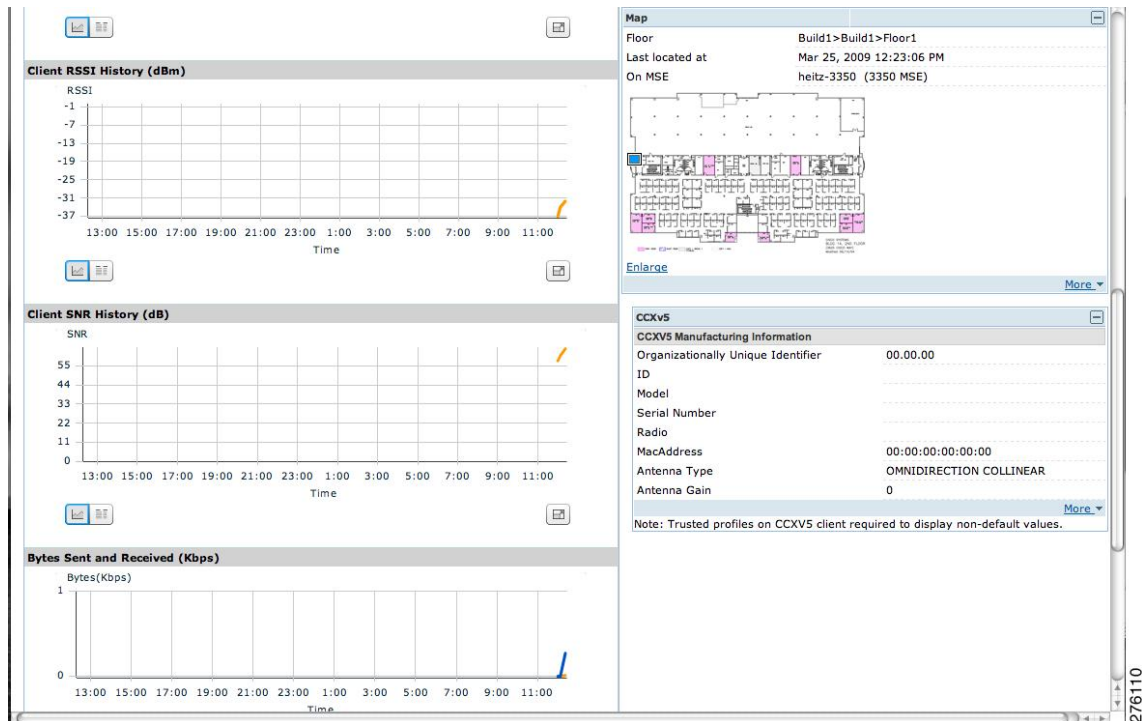
Step 5 Click the Client icon to see client details.

Figure 7: Client Details Page (1 of 2)

The screenshot displays the Cisco Wireless Control System interface for a client. The main section is titled "Client Details : Client 'unknown' - Cisco:b6:02:cf". Below this, there are several sections:

- Properties:** A table listing various client attributes such as Client User Name, IP Address, MAC Address, Vendor, CCX, Power Save, Controller, Port, Protocol, SSID, Profile Name, AP Name, AP IP Address, AP Type, AP Base Radio MAC, Interface, VLAN ID, 802.11 State, Security Policy, 802.11 Authentication, Encryption Cipher, EAP Type, RSSI, SNR (dB), Retries, Packets Tx/Rx, Bytes Tx/Rx, Policy errors, UpTime (Sec), Current TxRateSet, and Data RateSet.
- Association History:** A table showing recent client association entries with columns for Association Time, Duration, User Name, IP Address, AP Name, Controller Name, Map Location, SSID, Protocol, Traffic (MB), Hostname, and Roam Reason.
- Statistics:** A section for "Client AP Association History" featuring a graph showing association and disassociation events for AP AP001d.e554.0052 over a 24-hour period.
- Events:** A list of events, including "Location Changed" events with their respective dates and times.

Figure 8: Client Details Page (2 of 2)



Step 6 Click the **More** link to configure asset information for the client.

Monitoring Wireless Clients Using Search

Before You Begin

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**.

The Clients summary page 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. You can also filter the current list using the Show drop-down list.

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

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

To search for an MSE-located client using the Prime Infrastructure Advanced Search feature, follow these steps:

Step 1 Click **Advanced Search** located in the top right corner of the Prime Infrastructure UI.

Step 2 In the New Search dialog, choose **Clients** as the search category from the Search Category drop-down list.


Step 3 From the Media Type drop-down list, choose **Wireless Clients**.

Note The Wireless Type drop-down list appears only when you choose Wireless Clients as the media type.

- Step 4** From the Wireless Type drop-down list, choose any of the following types: **All**, **Lightweight**, or **Autonomous Clients**.
- Step 5** From the Search By drop-down list, choose **IP Address**.
- Note** Searching a client by IP address can contain either a full or partial IP address. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.
- Step 6** From the Clients Detected By drop-down list, choose **clients detected by MSE**.
This shows clients located by Context-Aware Service in the MSE by directly communicating with the Cisco WLCs.
- Step 7** From the Last detected within drop-down list, choose the time within which the client was detected.
- Step 8** Enter the client IP address in the Client IP Address text box. You can enter wither a partial or full IPv6 address.
- Note** If you are searching for the client from the Prime Infrastructure on the MSE by IPV4 address, enter the IPV4 address in the Client IP Address text box.
- Step 9** From the Client States drop-down list, choose the client states. The possible values for wireless clients are **All States**, **Idle**, **Authenticated**, **Associated**, **Probing**, or **Excused**. The possible values for wired clients are **All States**, **Authenticated**, and **Associated**.
- Step 10** From the Posture Status drop-down list, choose the posture status to know if the devices are clean or not. The possible values are **All**, **unknown**, **Passed**, and **Failed**.
- Step 11** Select the **CCX Compatible** check box to search for clients that are compatible with Cisco Client Extensions. The possible values are **All Versions**, **V1**, **V2**, **V3**, **V4**, **V5**, and **V6**.
- Step 12** Select the **E2E Compatible** check box to search for clients that are End to End compatible. The possible values are **All Versions**, **V1**, and **V2**.
- Step 13** Select the **NAC State** check box to search for clients identified by a certain Network Admission Control (NAC) state. The possible values are **Quarantine**, **Access**, **Invalid**, and **Not Applicable**.
- Step 14** Select the **Include Disassociated** check box to include clients that are no longer on the network but for which Prime Infrastructure has historical records.
- Step 15** From the **Items per page** drop-down list, choose the number of records to be displayed in the search results page.
- Step 16** Select the **Save Search** check box to save the selected search option.
- Step 17** Click **Go**.
The Clients and Users page appears with all the clients detected by the MSE.
-

Viewing the Clients Detected by the MSE

To view all the clients detected by MSE, follow these steps:

- Step 1** Choose **Monitor > Clients and Users** to view both wired and wireless clients information.
The Client and Users page appears.
- The Clients and Users table shows a few column by default. If you want to display the additional columns that are available, click  , and then click **Columns**. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.
- Step 2** Filter the current list to choose all the clients that are detected by MSE by choosing **Clients detected by MSE** from the Show drop-down list.

All the clients detected by MSE including wired and wireless appear. All the clients detected by MSE including wired and wireless appear.

The following different parameters are available in the Clients Detected by MSE table:

- MAC Address—Client MAC address.
 - IP Address—Client IP address.

The IP address that appears in the IP Address column is determined by a predefined priority order. The first IP address available in the following order appears in the IP address text box:

- IPv4 address

Note Only wireless clients have IPv6 addresses in this release. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

- IPv6 global unique address. If there are multiple addresses of this type, most recent IPv6 address that the client received is shown, because a user might have two Global IPv6 addresses but one might have been from an older Router Advertisement that is being aged out.
- IPv6 local unique address, if there are multiple then the most recent IPV6 local unique address is used by the client.
- IPv6 link local address. For an IPv6 address of the client which is self-assigned and used for communication before any other IPV6 address is assigned.

The following are the different IPv6 address types:

- Link-local Unicast—The link-local addresses are designed to be used for addressing on a single link for purposes such as auto-address configuration, neighbor discovery, or when no routers are present.
- Site-local Unicast—The site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix.
- Aggregatable Global Unicast—The aggregatable global unicast address uniquely identifies the client in global network and equivalent to public IPv4 address. A client can have multiple aggregatable global unicast addresses.

- IP Type—The IP address type of the client. The possible options are IPv4, IPv6, or Dual-stack that signifies a client with both a IPV4 and IPV6 addresses.
 - Global Unique
 - Unique Local
 - Link Local
- User Name—Username based on 802.1x authentication. Unknown is displayed for client connected without a username.
- Type—Indicates the client type.

- Vendor—Device vendor derived from OUI.
- Device Name—Network authentication device name. For example, WLC and switch.
- Location—Map location of the connected device.

- VLAN—Indicates the access VLAN ID for this client.
- Status—Current client status.
 - Idle—Normal operation; no rejection of client association requests.
 - Auth Pending—Completing a AAA transaction.
 - Authenticated—802.11 authenticated complete.
 - Associated—802.11 association complete. This is also used by wired clients to represent that a client is currently connected to the network.
 - Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.
 - To Be Deleted—The client is deleted after disassociation.
 - Excluded—Automatically disabled by the system due to perceived security threat.
- Interface—Cisco WLC interface (wireless) or switch interface (wired) that the client is connected to.
- Protocol
 - 802.11—Wireless
 - 802.3—Wired
- Association Time—Last association start time (for wireless client). For a wired client, this is the time when a client is connected to a switch port. This is blank for a client which is associated but has problems being on the network.
- CCX—Lightweight wireless only.
 - Select the radio button next to MAC Address in the Client and User page to view the associated client information. The following client parameters appear:
- Client attributes
- Client IPV6 Addresses
- Client Statistics
 - Note** Client Statistics shows the statistics information after the client details are shown.
- Client Association History
- Client Event Information
- Client Location Information
- Wired Location History
- Client CCX Information
- Client Attributes

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

- General—Lists the following information:

- User Name
- IP Address
- MAC address
- Vendor
- Endpoint Type
- Client Type
- Media Type
- Mobility Role
- Hostname
- E2E
- Foundation Service
- Management Service
- Voice Service
- Location Service

- Session—Lists the following information:

- Controller Name
- AP Name
- AP IP Address
- AP Type
- AP Base Radio MAC
- Anchor Address
- 802.11 State
- Association ID
- Port
- Interface
- SSID
- Profile Name
- Protocol
- VLAN ID
- AP Mode

- Security (wireless and Identity wired clients only)—Lists the following security information:
 - Security Policy Type
 - EAP Type
 - On Network
 - 802.11 Authentication
 - Encryption Cipher
 - SNMP NAC State
 - RADIUS NAC State
 - AAA Override ACL Name
 - AAA Override ACL Applied Status
 - Redirect URL
 - ACL Name
 - ACL Applied Status
 - FlexConnect Local Authentication
 - Policy Manager State
 - Authentication ISE
 - Authorization Profile Name
 - Posture Status
 - TrustSec Security Group
 - Windows AD Domain
- Note** The identity clients are clients whose authentication type is 802.1x, MAC Auth Bypass, or Web Auth. For non-identity clients, the authentication type is N/A.
- Note** The data that appears under the client attributes differs based on identity and non-identity clients. For identity clients, you can see the security information such as Authentication status, Audit Session ID, and so on.

- Statistics (wireless only)
- Traffic—Shows the client traffic information.
- For wireless clients, client traffic information comes from the Cisco WLC. For wired clients, the client traffic information comes from the ISE, and you must enable accounting information and other necessary functions on the switches.

Statistics

The **Statistics** group box contains the following information for the selected client:

- Client AP Association History.

- Client RSSI History (dBm)—History of RSSI (Received Signal Strength Indicator) as detected by the access point with which the client is associated.
- Client SNR History—History of SNR (signal-to-noise ratio of the client RF session) as detected by the access point with which the client is associated.
- Bytes Sent and Received (Kbps)—Bytes sent and received with the associated access point.
- Packets Sent and Received (per sec)—Packets sent and received with the associated access point.
- Client Data rate

This information is presented in interactive graphs.

Client IPV6 Addresses

The Client IPv6 Address group box contains the following information for the selected client:

- IP Address—Shows the client IPv6 address.
- Scope—Contains 3 scope types: Global Unique, Local Unique, and Link Local.
- Address Type—Shows the address type.
- Discovery Time—Time when the IP was discovered.

Association History

The association history group box shows information regarding the last ten association times for the selected client. This information helps in troubleshooting the client.

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

Events

The Events group box in the Client Details page displays all events for this client including the event type as well as the date and time of the event:

- Event Type
- Event Time
- Description

Map

Click **View Location History** to view the location history details of wired and wireless clients.

The following location history information is displayed for a wired or wireless client:

- Timestamp
 - State
 - Port Type
 - Slot
 - Module
 - Port
 - User Name
 - IP Address
 - Switch IP
 - Server Name
 - Map Location Civic Location
-

Configuring Buildings

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

- [Adding a Building to a Campus Map](#), on page 209
- [Viewing a Building](#), on page 126
- [Editing a Building](#), on page 127
- [Deleting a Building](#), on page 127
- [Moving a Building](#), on page 128

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:

- a) Enter the building name.
- b) Enter the building contact name.
- c) Enter the number of floors and basements.
- d) Enter the horizontal position (distance from the corner of the building rectangle to the left edge of the campus map) and the vertical position (distance from the corner of the building rectangle to the top edge of the campus map) in feet.

Note To change the unit of measurement (feet or meters), choose **Monitor > Site Maps** and choose **Properties** from the Select a command drop-down list.
- e) Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.

Note

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

Tip You can also use **Ctrl-click** to resize the bounding area in the upper-left corner of the campus map. As you change the size of the bounding area, the Horizontal Span and Vertical Span parameters of the building change to match your actions.
- f) Click **Place** to put the building on the campus map. The Prime Infrastructure creates a building rectangle scaled to the size of the campus map.
- g) Click the building rectangle and drag it to the desired position on the campus map.

Note After adding a new building, you can move it from one campus to another without having to recreate it.
- h) Click **Save** to save this building and its campus location to the database. The 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:
- Enter the building name.
 - 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.
 - Enter the number of floors and basements.
 - 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.
 - Click **OK** to save this building to the database.
- Step 4** (Optional) To assign location presence information for the new building, do the following:
- Choose **Location Presence** from the Select a command drop-down list. Click **Go**. The Location Presence page appears.
 - 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, country, 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.
 - 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, on page 209](#) for more information.
 - Edit Building—See the [Editing a Building, on page 127](#) for more information.
 - Delete Building—See the [Deleting a Building, on page 127](#) 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.

- [Monitoring Tags Using Maps](#), on page 214
- [Monitoring Tags Using Search](#), on page 214
- [Overlapping Tags](#), on page 216

Monitoring Tags Using Maps

On an 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 > 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.
Note Do not click **Save Settings** unless you want to save changes made to the floor settings across all maps.
- 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 (Cisco WLC 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
- Cisco WLC 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 tags, follow these steps:

- Step 1** Choose **Monitor > Tags**. The Tag Summary page appears.
- Step 2** To view a summary of tags associated with a specific MSE, click the **Total Tags** link.
Note If the listing of MSEs or tags is lengthy, you can use Search or Advanced Search to isolate a specific tag.
- 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.
- In the Advanced Search pane, select **Tags** as the search category.
 - Select the additional tag search criteria.
 - 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 23: 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; Cisco WLC or MSEs; Floor Area, or Outdoor Area. Note The MSE search includes both location servers and MSEs.
Search in (Tier 2 search criteria)	—	MSEs or Prime Infrastructure or Cisco WLCs. Note The Prime Infrastructure controller option indicates that the search for Cisco WLC is done within the Prime Infrastructure. Note The MSE search includes both location servers and MSEs.
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 tabs by (Tier 1 search) value.	If the Search for tags by value is the following: Asset Name, then enter tag asset name. Asset Category, then enter tag asset category. Asset Group, then enter tag asset group. MAC Address, then enter tag MAC address. Controller, then select controller IP address. MSEs, then choose an MSE IP address from drop-down list. Floor Area, then choose campus, building, and floor area. Outdoor Area, then choose campus and outdoor area.	

Search Criteria	Variable Search Criteria	Possible Values
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 an 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.

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 Cisco WLC, 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 Geo-Location

The MSE provides physical location of wired clients, wired endpoints, switches, Cisco WLCs, and access points present in a wireless network deployment. Currently, MSE provides location information in geo-location format to the external entities through northbound and southbound entities.

To improve the accuracy of the geo-location information provided by MSE, this feature aims to transform the geometric location co-ordinates of a device to geo-location coordinates (latitude and longitude) and provides it to the external entities through northbound and southbound interfaces.



Note At least three GPS markers are required for geo-location calculation. The maximum number of GPS markers that you can add is 20.

- [Adding a GPS Marker to a Floor Map, on page 217](#)
- [Editing a GPS Marker, on page 218](#)
- [Deleting a GPS Marker From the Floor, on page 218](#)

Adding a GPS Marker to a Floor Map

To add a GPS marker to a floor map, follow these steps:

-
- Step 1** Choose **Monitor > Site Maps** to display the Maps page.
- Step 2** Choose **Campus Name > Building Name > Floor Name**.
- Step 3** Choose the **Add/Edit GPS Markers** Information menu option on the top left menu to open the Add/Edit GPS page. A GPS Marker icon appears on the top left corner of the map (X=0 Y=0).
- Step 4** You can drag the GPS Marker icon and place it in the desired location on the map or enter the X and Y position values in the GPS Marker Details table on the left sidebar menu to move the marker to the desired position.
- Note** If the markers added are too close, then the accuracy of geo-location information is less.
- Step 5** Enter the Latitude and Longitude degrees for the selected GPS Marker icon in the left sidebar menu.
- Step 6** Click **Save**.
The GPS Marker information is saved to the database.
- Step 7** Click **Apply to other Floors of Building** to copy GPS markers on one floor of a building to all the remaining floors of that building.
-

Editing a GPS Marker

To edit a GPS marker present on the floor, follow these steps:

-
- Step 1** Choose **Monitor > Site Maps** to display the Maps page.
 - Step 2** Choose **Campus Name > Building Name > Floor Name**.
 - Step 3** Choose the **Add/Edit GPS Markers Information** menu option to open the Add/Edit GPS page.
 - Step 4** Select an existing GPS Marker which is present on the floor from the left sidebar menu.
 - Step 5** From the left sidebar menu, you can change the Latitude, Longitude, X Position, and Y Position which is associated with the GPS marker.
 - Step 6** Click **Save**.
The modified GPS marker information is now saved to the database.
-

Deleting a GPS Marker From the Floor

To delete a GPS marker from the floor, follow these steps:

-
- Step 1** Choose **Monitor > Site Maps** to display the Maps page.
 - Step 2** Choose **Campus Name > Building Name > Floor Name**.
 - Step 3** Choose the **Add/Edit GPS Markers Information** menu option to open the Add/Edit GPS page.
 - Step 4** Select an existing GPS marker that is present on the floor from the left sidebar menu.
Note You can delete multiple GPS markers present on a floor by selecting the **Multiple GPS Markers** check box.
 - Step 5** Click **Delete GPS Marker**.
The selected GPS marker is deleted from the database.
-

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.
 - Choose **Chokepoint** as the search category.
 - 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.
 - Enter either the chokepoint name or MAC address.
 - 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**.

If no match exists, a message appears in the Search Results page.
-

Ekahau Site Survey Integration

Ekahau Site Survey (ESS) tool is used for designing, deploying, maintaining, and troubleshooting high performance Wi-Fi networks. ESS works over any 802.11 network and is optimized for centrally managed 802.11n Wi-Fi networks.

You can use the ESS tool to import the existing floor maps from the Prime Infrastructure and export the project to the Prime Infrastructure. For more information, see the Cisco Prime Infrastructure Integration section in the ESS online help.



Note The Prime Infrastructure site survey calibration requires that you have collected at least 150 survey data points at 50 distinct locations. If you do not have enough survey data points, a warning is given when trying to export the survey data.



Note If there are no access points in the Prime Infrastructure during the site survey, the site survey will not happen.



Note If the floor map scales are incorrect in the Prime Infrastructure, the visualizations in the ESS will be distorted.

AirMagnet Survey and Planner Integration

AirMagnet survey and AirMagnet planner is integrated with the Cisco Prime Infrastructure. This integration increases the operational efficiencies by eliminating the need to repeat the wireless planning and site survey tasks commonly associated with deployment and management of wireless LAN networks.

The AirMagnet survey tool allows you to export real world survey data to the Prime Infrastructure for calibrating planner modeling. With the AirMagnet planner, you can create and export planner projects directly to the Prime Infrastructure. This enables the Prime Infrastructure to create its own project directly from the imported AirMagnet Planner tool. For more information, see the AirMagnet Survey and Planning documentation which is available at Fluke Networks website.

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).

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.

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.

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 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 MSE 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 MSE 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).

- 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 Interferers

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:

- 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 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, on page 92](#).

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, severity greater than or equal to 5 are displayed in the AP Detected Interferers page.

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.
-

Clustering of Monitor Mode APs Using MSE

Where *value* is the distance in feet for clustering. The default value is 150.



Performing Maintenance Operations

This chapter describes how to back up and restore Cisco Mobility Services Engine (MSE) data and how to update the MSE software. It also describes other maintenance operations.

- [Guidelines and Limitations, page 227](#)
- [Recovering a Lost Password, page 227](#)
- [Recovering a Lost Root Password, page 228](#)
- [Backing Up and Restoring Mobility Services Engine Data, page 228](#)
- [Configuring the NTP Server, page 232](#)
- [Resetting the System, page 232](#)
- [Clearing the Configuration File, page 232](#)

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**.
 - Step 4** At the end of the line, insert a space, followed by the number one (1). Press **Enter** to save this change.
 - Step 5** Press **b** to begin boot.

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

- Step 6** Enter the **passwd** command to change the root password.
- Step 7** Enter and confirm the new password.
- Step 8** 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**.
- Step 4** At the end of the line, enter a space, followed by the number one (**1**). Press **Enter** to save this change.
- Step 5** 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 6** Enter the **passwd** command to change the root password.
- Step 7** Enter and confirm the new password.
- Step 8** Restart the machine.
- Note** Ensure that you remember the root password and only change the password if it is absolutely necessary.
-

Backing Up and Restoring Mobility Services Engine Data

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

This section contains the following topics:

- [Backing Up Mobility Services Engine Historical Data](#), on page 229
- [Restoring Mobility Services Engine Historical Data](#), on page 229
- [Enabling Automatic Location Data Backup](#), on page 230
- [Downloading Software to the Mobility Services Engines](#), on page 230
- [Manually Downloading Software](#), on page 231

Backing Up Mobility Services Engine Historical Data

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 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 backup; (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 other the Prime Infrastructure page. Backups are stored in the FTP directory you specify during the Prime Infrastructure installation.
-

Restoring Mobility Services Engine Historical Data

You can use Prime Infrastructure to restore backed up historical data.

To restore mobility services engine data, follow these steps:

-
- Step 1** Choose **Services > Mobility Services**.
 - Step 2** Click the name of the MSE that you want to restore.
 - Step 3** Choose **System > Maintenance**.
 - Step 4** Click **Restore**.
Enter the FTP server address.
 - 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 MSE.
This option is applicable for network designs, wired switches, Cisco WLCs, and event definitions. The existing location history data is retained, however, you must use manual service assignments to perform any future location calculations.
 - Step 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, Prime Infrastructure displays a message to that effect.
- Note** You should not work on other MSE 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 MSE 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 MSE.
 - Step 7** After the image is transferred to the MSE, log in to the MSE 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 Prime Infrastructure, follow these steps to upgrade the software manually using a local (console) or remote (SSH) connection:

Step 1

Transfer the new MSE image onto the hard drive.

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

Note The MSE image is compressed at this point.

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

Your entries should look like this example:

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

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

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

```
gunzip CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz
The decompression yields a bin file.
```

- d) Make sure that the CISCO-MSE-L-K9-x-x-x-x-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 MSE.

Step 3

Log in as root and enter the following command:

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

Step 4

To install the new MSE image, enter the following command:

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

Step 5

Start the new MSE 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 MSE:

```
/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

**Note**

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](#), on page 59.

Clearing the Configuration File

For information on clearing the configuration file, see the [Clearing the System Database](#), on page 59.



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 endpoints.

This chapter contains the following sections:

- [Setup Wizard Update](#), page 233
- [Certificate Management](#), page 235
- [Updated Open Port List](#), page 242
- [Syslog Support](#), page 242
- [MSE and RHEL 5](#), page 242

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](#)
- [Configuring the Remote Syslog Server to Publish MSE Logs](#)
- [Configuring the Host Access Control Settings](#)

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. (Rewrite the config command option for the entire section after this)

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: 283.12.13.4

Configure Remote Syslog Server Priority parameter.
select a priority level
1)ERROR (ERR)
2)WARNING
3)INFO
Enter a priority level (1-3) :2
Configure Remote Syslog Server's Facility parameter.
Select a logging facility
  KERN(0), // Kernel messages
  USER(1), // user-level messages
  MAIL(2), // mail system
  DAEMON(3), // system daemons
  AUTH(4), // security/authorization messages (note 1)
  SYSLOG(5), // messages generated internally by syslogd
  LPR(6), // line printer subsystem
  NEWS(7), // network news subsystem
  UUCP(8), // UUCP subsystem
  CRON(9), // clock daemon (note 2)
  SECURITY(10), // security/authorization messages (note 1)
  FTP(11), // FTP daemon
  NTP(12), // NTP subsystem
  LOGAUDIT(13), // log audit (note 1)
  LOGALERT(14), // log alert (note 1)
  CLOCK(15), // clock daemon (note 2)
  LOCAL0(16), // local use 0 (local0)
  LOCAL1(17), // local use 1 (local1)
  LOCAL2(18), // local use 2 (local2)
  LOCAL3(19), // local use 3 (local3)
  LOCAL4(20), // local use 4 (local4)
  LOCAL5(21), // local use 5 (local5)
  LOCAL6(22), // local use 6 (local6)
  LOCAL7(23); // local use 7 (local7)

Enter a facility(0-23) :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](#)
- [Importing the CA Certificate](#)
- [Importing Server Certificate](#)
- [Enabling or Disabling Client Certificate Validation](#)
- [Configuring Online Certificate Status Protocol \(OCSP\) Settings](#)
- [Importing a CRL](#)
- [Clearing Certificate Configuration](#)
- [Showing Certificate Configuration](#)

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's website to generate a CA certificate.

Example:

```
Certificate Management Options
  1: Import CA Certificate
  2: Import Server Certificate
  3: Enable Client Certificate Validation
  4: Disable Client Certificate Validation
  5: OCSP Settings
  6: Import a CRL
  7: Create a CSR (Certificate Signing request)
  8: Clear Certificate Configuration
  9: Show Certificate Configuration
 10: Exit
Please enter your choice (1-10)
7
Enter the directory in which the CSR needs to be stored:/root/TestFolder
Enter the Keysize: 2048
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/root/TestFolder/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/mseservercsr.pem
The Private key is in: /root/TestFolder/mseserverkey.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 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: OCSP Settings
6: Import a CRL
7: Create a CSR (Certificate Signing request)
8: Clear Certificate Configuration
9: Show Certificate Configuration
10: Exit
Please enter your choice (1-10)
3
Enabling client certificate validation done

Certificate Management Options
1: Import CA Certificate
2: Import Server Certificate
3: Enable Client Certificate Validation
4: Disable Client Certificate Validation
5: OCSP Settings
6: Import a CRL
7: Create a CSR (Certificate Signing request)
8: Clear Certificate Configuration
9: Show Certificate Configuration
10: Exit
Please enter your choice (1-10)
3
Enabling client certificate validation done

```

Configuring Online Certificate Status Protocol (OCSP) Settings

Use this option to configure the Online Certificate Status Protocol (OCSP) settings. You are prompted to enter the OCSP URL and default name. In other words, you are asked to provide the URL and default name for the certificate authority.

Example:

```

Certificate Management Options
  1: Import CA Certificate
  2: Import Server Certificate
  3: Enable Client Certificate Validation
  4: Disable Client Certificate Validation
  5: OCSP Settings
  6: Import a CRL
  7: Create a CSR (Certificate Signing request)
  8: Clear Certificate Configuration
  9: Show Certificate Configuration
 10: Exit
Please enter your choice (1-10)
5
Enter the OCSP URL :
http://ocsp.227.104.178.224
Enter the default ocsp name :ExampleServer

```

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: 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)
9

Certificate Nickname                                     Trust Attributes
                                                         SSL,S/MIME,JAR/XPI

CA-Cert1296638915                                     CT,,
Server-Cert                                           u,u,u
=====
***** Certificates in the database *****
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      74:a1:38:25:75:94:a5:9a:43:2d:4a:23:bd:82:bc:e5
    Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
    Issuer: "CN=ROOTCA1"
    Validity:
      Not Before: Tue Nov 16 18:49:25 2010
      Not After : Mon Nov 16 18:59:25 2015
    Subject: "CN=ROOTCA1"
    Subject Public Key Info:
      Public Key Algorithm: PKCS #1 RSA Encryption
      RSA Public Key:
        Modulus:
          da:06:43:70:56:d8:41:ec:69:e6:65:ad:c5:3b:04:0b:
          cb:cd:83:7c:5f:6e:8f:aa:17:50:6b:6a:3a:48:35:a6:
          65:8a:47:91:48:2f:93:2b:d8:53:6b:33:5c:a9:c2:b2:
          33:c2:fc:9c:55:25:19:d0:79:23:3f:66:60:24:04:ce:
          a3:08:c7:60:f0:b0:8d:b1:31:71:f5:b9:3f:17:46:1a:
          fd:3d:c9:3b:9f:bf:fe:a3:8d:13:52:aa:6b:59:80:43:
          f8:24:e7:49:10:ca:54:6c:f7:aa:77:04:4b:c2:3f:96:
          8d:a1:46:e8:16:1e:a8:e6:86:f4:5c:a0:e5:15:eb:f8:
          5a:72:97:f9:09:65:84:f6:a5:0b:a3:c6:ab:a9:9e:61:
          07:5a:8d:b1:af:93:3b:68:53:8a:5d:f0:14:6e:02:e4:
          38:d2:31:29:5e:a2:1a:93:de:a0:bd:44:9b:05:fd:7b:
          5f:59:23:a1:47:97:87:84:dd:0e:9f:0a:09:cd:df:34:
          b9:6f:9c:b5:4d:07:23:8b:a5:27:16:cd:75:5a:6e:f1:
          c1:5b:6b:21:3a:fd:d9:4d:72:b4:d6:dc:37:86:c2:e3:
          60:56:69:3c:52:27:19:bf:4c:0c:ea:6e:34:29:8c:cf:
          17:50:b3:31:cc:86:1e:32:dc:40:58:92:26:88:58:63
        Exponent: 65537 (0x10001)
    Signed Extensions:
      Name: Certificate Key Usage
      Usages: Digital Signature
              Certificate Signing
              CRL Signing
```

```

Name: Certificate Basic Constraints
Critical: True
Data: Is a CA with no maximum path length.

Name: Certificate Subject Key ID
Data:
    30:89:49:06:62:fe:6c:29:75:bc:90:8b:a5:6a:87:f8:
    8e:61:49:eb

Name: Microsoft CertServ CA version
Data: 0 (0x0)

Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
Signature:
    d6:35:b9:27:1f:5b:1a:12:9d:41:a3:16:3a:3a:08:ba:
    91:f4:a9:4b:1b:ff:71:7c:4e:74:16:36:05:04:37:27:
    d0:73:66:a2:47:50:0d:b3:fa:b1:34:dc:36:b8:a9:0a:
    2d:5c:84:35:30:51:4f:7b:55:47:00:53:73:40:c8:95:
    a9:82:83:32:06:ed:0c:95:6d:b1:13:08:3a:e3:cc:88:
    40:9f:e6:43:8c:36:88:e4:a1:91:3e:20:74:29:bf:91:
    25:c1:ef:bc:10:bb:cb:be:08:2c:64:2d:41:a1:3f:81:
    48:ed:80:ed:97:68:6d:83:30:e2:c8:90:ce:45:3a:45:
    cc:78:3c:c4:af:62:73:6a:29:60:c7:70:b1:4c:84:43:
    77:2d:9c:b9:13:dc:9c:b5:8c:74:62:7b:8e:41:ed:37:
    b8:2c:c0:3b:0c:49:cf:61:40:cc:2c:22:74:b2:6b:50:
    e8:31:c9:5f:b8:04:dd:39:7a:9a:46:5e:ee:5a:e8:6a:
    4b:75:97:69:7e:fc:7f:9d:9f:df:f0:3f:06:62:79:77:
    d9:a8:49:a6:00:bf:93:61:00:aa:55:11:26:92:f4:c2:
    8a:61:21:80:af:ef:ab:22:11:ee:10:79:15:4b:1a:8f:
    ae:55:c5:61:03:8e:db:1a:3e:5a:6f:a6:6d:3e:5b:a4
Fingerprint (MD5):
    31:54:A0:D3:A7:40:1A:1E:95:8E:8A:D9:EC:70:47:35
Fingerprint (SHA1):
    F5:72:62:5C:46:AB:2A:5D:7A:75:DA:CB:44:E6:38:76:E0:9E:17:C3

Certificate Trust Flags:
SSL Flags:
    Valid CA
    Trusted CA
    Trusted Client CA
Email Flags:
Object Signing Flags:

Certificate:
Data:
    Version: 3 (0x2)
    Serial Number:
        4d:a9:34:de:00:00:00:00:00:0b
    Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
    Issuer: "CN=ROOTCA1"
    Validity:
        Not Before: Wed Feb 02 22:40:44 2011
        Not After : Thu Feb 02 22:50:44 2012
    Subject: "E=abc@example.com,CN=abc-mse,OU=XYZ,O=Companyo,L=City,S
        T=State,C=IN"
    Subject Public Key Info:
        Public Key Algorithm: PKCS #1 RSA Encryption
        RSA Public Key:
            Modulus:
                a8:7b:2f:57:94:53:fc:90:c9:37:cb:9a:b3:f6:f4:b8:
                02:04:f3:f8:d8:e1:d1:23:d4:62:7b:30:05:d2:b0:da:
                17:88:b0:22:d5:a6:04:c6:66:fc:64:54:ff:78:5b:f9:
                ef:05:3a:3e:ec:b8:01:7c:3c:9b:78:ac:1d:7f:fb:3b:
                39:f5:31:d2:a2:27:d8:d1:ee:2e:77:98:04:bb:7c:f6:
                0b:9c:ea:15:12:cf:3d:1c:b8:57:63:df:2b:00:48:25:
                32:e4:58:9a:e1:ff:80:5d:2c:24:75:e2:06:de:e6:ae:
                03:7e:c5:f6:e7:97:4d:c1:ad:19:4f:47:20:6c:8d:7a:
                60:75:85:34:3e:ed:f3:1a:77:65:e2:7a:18:e1:17:3d:
                bd:62:1a:1c:4a:d9:49:c3:93:2e:6a:69:fc:e8:87:1e:
                dc:69:11:63:f1:17:63:41:e4:8d:1e:19:3c:e8:80:a9:
                6b:04:c8:18:fb:c9:fe:9d:77:71:30:d2:87:46:82:49:
                0a:1d:ed:4d:ad:66:ad:65:6f:fb:b2:6a:31:45:33:59:
                a7:04:3a:2d:72:f7:55:02:fa:99:02:d9:dd:5e:21:4b:

```



```

                2c:c9:3e:cc:a4:a0:dd:4c:4f:7f:be:45:a7:dd:a9:c4:
                ad:bc:a9:25:a6:1f:53:b8:d0:98:4a:b7:c3:41:a3:d7
                Exponent: 65537 (0x10001)
Signed Extensions:
  Name: Certificate Subject Key ID
  Data:
    bc:a3:66:c6:19:07:56:0a:90:7a:b1:1a:ea:37:17:20:
    74:b8:f1:f5

  Name: Certificate Authority Key Identifier
  Key ID:
    30:89:49:06:62:fe:6c:29:75:bc:90:8b:a5:6a:87:f8:
    8e:61:49:eb

  Name: CRL Distribution Points
  URI: "http://win-bncnizib5e2/CertEnroll/ROOTCA1.crl"
  URI: "file://WIN-BNCNIZIB5E2/CertEnroll/ROOTCA1.crl"

  Name: Authority Information Access
  Method: PKIX CA issuers access method
  Location:
    URI: "http://win-bncnizib5e2/CertEnroll/WIN-BNCNIZIB5E2_ROOTC
    Al.crt"
  Method: PKIX CA issuers access method
  Location:
    URI: "file://WIN-BNCNIZIB5E2/CertEnroll/WIN-BNCNIZIB5E2_ROOTC
    Al.crt"

Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
Signature:
aa:13:74:0d:d1:8c:85:cc:3d:8f:35:c7:e5:9b:a6:4c:
f8:8b:12:a0:12:9f:dc:0a:0a:b5:40:12:eb:05:a9:2b:
65:c5:a3:22:62:1f:47:cd:dd:0f:b8:03:11:a5:63:23:
64:a7:f8:8b:ec:d4:21:dc:d8:22:de:52:75:d9:fb:23:
d4:14:35:d8:78:b7:e2:23:75:05:b4:d0:09:e0:55:ec:
96:8c:22:23:fb:86:74:71:69:ac:03:57:b6:ec:14:a9:
f9:99:b3:98:4c:00:69:e2:26:f8:7b:e9:a0:2a:c2:f4:
6a:75:fc:d1:08:d6:5b:76:93:7a:2c:21:8b:83:ab:52:
a0:85:16:f1:38:35:01:8d:21:34:60:b7:82:39:a7:42:
e7:5f:1a:b7:9d:bf:54:ee:27:97:ba:f8:ca:31:d4:35:
67:55:36:02:b4:48:ab:16:ee:0f:65:56:48:51:de:aa:
9f:7d:35:9b:eb:58:3a:0c:4a:8a:ae:3a:18:47:e3:11:
7b:82:b3:fb:88:94:df:85:82:23:0b:07:46:12:2c:d0:
dd:a7:91:c0:e1:4c:e7:38:9e:34:30:9b:b6:db:c6:8d:
03:df:6e:6b:27:76:da:31:50:44:cd:c8:21:30:42:3c:
75:dc:99:d2:6b:91:9e:bd:b0:5c:8a:52:6b:92:41:0f
Fingerprint (MD5):
77:73:3C:D6:B9:2E:F2:AA:C4:A6:7E:9F:60:D7:55:F7
Fingerprint (SHA1):
60:F8:DC:D2:75:BA:D9:35:4D:21:60:CA:90:EF:09:67:FF:D0:DC:CF

Certificate Trust Flags:
  SSL Flags:
    User
  Email Flags:
    User
  Object Signing Flags:
    User

***** CRLs in the database *****
None
***** Client Certification Settings *****
Client Certificate Validation is disabled
***** OCSP Setting *****
OCSP URL :
http://ocsp.227.104.178.224
OCSP nick name :ExampleServer
=====

```

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. The syslog for wIPS is located at `/opt/mse/logs/wips`. This log contains information about wIPS Service, Service start/stop logs, DB logs and error logs. For detailed debug logs, you should turn on `MAJOR_DEBUG` on the wIPS logs .

MSE and RHEL 5

The MSE OS is based on Red Hat Enterprise Linux (RHEL) 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 4.3p2-82.el5(which addresses the vulnerabilities in 4.3p2-26.el5_2.1).



INDEX

A

- adding [67, 69](#)
- alarm notifications [165](#)
 - emailing [165](#)
- AP Location data [145](#)
- automatic backup [230](#)
- automatic synchronization [22](#)

B

- backup historical data [229](#)
- buildings [125](#)
 - adding to PI database [125](#)

C

- certificate management [235](#)
- civic address [125](#)
- clear [165](#)
- configuring [167, 232](#)

D

- deleting [68, 70](#)
- download [168](#)

E

- edit location presence information [124](#)
- edited saved marker [177](#)
- editing [49](#)
- editing scheduled run details [176](#)

F

- failover [29](#)

G

- GPS markers [125](#)

H

- high availability [27](#)

I

- identity client [207](#)

L

- location presence [124](#)
 - assigning [124](#)

M

- mesh parent-child hierarchical view [139](#)

N

- network designs [17](#)

O

- out-of-sync [23](#)

P

pairing matrix [28](#)
permission [69](#)
properties [70](#)

R

recovering lost [227](#)
restore historical data [229](#)

S

saved [177](#)
software download [230](#)
statistics [107](#)
synchronization [23](#)
synchronization history [24](#)

V

viewing [162, 163, 166](#)
viewing HA parameters [43](#)
viewing HA status [43](#)