Cisco Mobility Services Engine and Services

Overview of Cisco Mobility Services Engine (MSE)

The Cisco MSE supports various services within the overall Cisco Unified Wireless Network (CUWN).

The Cisco MSE currently supports the following services:

- Location Service—Also known as Context Aware Service (CAS). This is the core service of the MSE that turns on Wi-Fi client tracking and location API functionality. Allows MSE to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as presence, location, telemetry data, and historical information.
- Wireless Intrusion Protection Service—Provides wireless-specific network threat detection and mitigation against malicious attacks, security vulnerabilities, and sources of performance disruption within the CUWN infrastructure. wIPS visualizes, analyzes, and identifies wireless threats, and centrally manages mitigation and resolution of security and performance issues using Cisco monitor mode and Enhanced Local Mode (ELM) Access Points. Proactive threat prevention is also supported to create a hardened wireless network core that is impenetrable by most wireless attacks.
- Mobile Concierge—Mobile Concierge enables the Cisco Mobility Services Advertisement Protocol (MSAP). This protocol enables direct communication between the MSE and mobile devices, allowing

content to be pushed directly to the mobile device pre-association. This functionality is dependent on the mobile device supporting 802.11u and MSAP.

- CMX Analytics Service—The CMX Analytics service analyzes wireless device location information in a particular network. The CMX Analytics service uses the data provided by the MSE to calculate the location of Wi-Fi devices in the Wireless Local Area Network (WLAN). In addition, the FastLocate feature sends information about the RSSI strength of data packets to the Cisco WLC that can be used for location calculations.

When a wireless device is enabled in a network, it transmits probe request packets to identify the wireless network in its neighborhood. Even after connecting to the access point in the WLAN, the client devices continue to transmit probe request packets to identify other access points for better quality of service. The access points gather these request and the associated RSSI from the various wireless devices and forwards them to the Wireless LAN Controller (WLC). The controller then forwards this information to the MSE.

The basic data that is collected from various APs, when analyzed, produces information and knowledge about the movement and behavior patterns of people who are using Wi-Fi devices in the building. For example, the building can be an airport, shopping mall, city center, and so on. The CMX Analytics service helps the airport authorities or the building owners to understand the movement of passengers or customer within their building. This helps them improve the signage, make changes to the under utilized areas, and so on.

Related Topics

Add MSEs to Cisco Prime Infrastructure, on page 2
Cisco Prime Infrastructure Data That is Synchronized With MSE, on page 8
Configure Mobile Concierge Using MSE, on page 61

Add MSEs to Cisco Prime Infrastructure

You can add an 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 the MSE. If you launch the wizard with an existing MSE for configuration, then the Add MSE option appears as Edit MSE Details.

To add an MSE to Prime Infrastructure, log in to Prime Infrastructure and follow these steps:

Before you begin

- To learn more about Cisco Adaptive wIPS features and functionality, go to https://www.cisco.com/to watch a multimedia presentation. Here you can find the learning modules for a variety of Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.
- Prime Infrastructure recognizes and supports the MSE 3355 appropriately. You can access the MSE installation guide at https://www.cisco.com/c/en/us/td/docs/wireless/mse/3355/user/guide/mse3355_qsg/mse_qsgmain.html.
- The **Services > Mobility Services > Mobility Services Engines** page is available only in root virtual domain.

Procedure

Step 1 Verify that you can ping the mobility service engine that you want to add from Prime Infrastructure.

Step 2 Choose **Services** > **Mobility 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**.

The Add Mobility Services Engine page appears.

Step 4 Enter the following information:

- Device Name—User-assigned name for the MSE.
- IP Address—The IP address of the mobility service engine.

An MSE is added only if a valid IP address is entered. The Device Name helps you distinguish between devices if you have multiple Prime Infrastructure with multiple mobility services engines, but it is not considered when validating an MSE.

- Contact Name (optional)—The mobility service engine administrator.
- Username—The default username is admin. This is the Prime Infrastructure communication username configured for MSE.
- Password—The default password is admin.This is the Prime Infrastructure communication password configured for MSE.

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.

- 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, controllers, and event definitions. The existing location history data is retained, however you must use manual service assignments to perform any future location calculations.

Step 5 Click **Next**.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.

Configuring Services for MSE

Step 6 To enable a service on the MSE, select the check box next to the service. The different type of services are:

- 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.
- WIPS—The Wireless Intrusion Prevention System check box, it detects wireless and performance threats.
- Mobile Concierge Service—The Mobile Concierge Service check box, it provides service advertisements that describe the available services for the mobile devices.
- CMX Analytics Service—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.
- CMX Connect & Engage—The CMX Connect and Engage service provides a guest Wi-Fi onboarding solution, as well as zone and message configuration for the CMX Software Development Kit (SDK).

- HTTP Proxy Service—The HTTP Proxy service on the MSE terminates all HTTP traffic intercepted using Policy Based Routing (PBR) and acts as a forward proxy by pulling contents on behalf of wireless clients.

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

Configuring MSE Tracking and History Parameters

Step 7 After you enable services on the MSE, the Select Tracking & History Parameters page appears.

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

Step 8 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 9 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 10 Click Next to Assign Maps to the MSE.

Assigning Maps to the MSE

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

Step 11 Once you configure MSE tracking and history parameters, the Assigning Maps page appears.

The Assign Maps page shows the following information:

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

Step 12 You can see the required map type by selecting either All, Campus, Building, Floor Area, or Outdoor Area from the Filter option available on the page.

Step 13 To synchronize a map, select the **Name** check box, and click **Synchronize**.

Upon synchronization of the network designs, the appropriate controllers that have APs assigned on a particular network design are synchronized with the MSE automatically.

Step 14 Click Next to configure mobile app enablement.

Mobile App Enablement

Enabling this integration will allow the MSE to send floor maps and wireless client position notification to Meridian. Meridian used this information to provide location-based services to your users without requiring them to connect to your network and access the MSE directly. After enabling Meridian, you will receive an e-mail with instructions on how to activate your account and share access with others in your organization. You can utilize Meridians platform to provide location services to your visitors either through the Meridian mobile app or your own apps using their mobile SDKs for Android and iOS. The data bandwidth for each wireless client position or zone notification from MSE to Meridian can be maximum of 1 MB/second.

Once you assign maps to the MSE, the Mobile App Enablement page appears.

Step 15 Select the **Enable Mobile App Integration** check box to enable the mobile application integration. You can click an icon to open the Mobile App Enablement Help page.

Step 16 Enter the name for the location on the **Location Name** text box. The name you enter here will appear in the Meridian app so that you can try out the location services on your own device.

Step 17 Enter the email address in the **E-mail Address** text box to access the Meridian online editor and SDK. Meridian will email these addresses with instructions on how to access your account and share it with others in your organization.

Step 18 Enter the server where the MSE can register its UDI and send the maps that are synchronized to the MSE in the**Registration Endpoint** text box.

Step 19 Enter the server detail where the MSE can send location update notifications in the data format specified in the **Notifications Endpoint** text box.

Step 20 Select the **Notifications Data Format** radio button. This is the data format of the notifications sent from the MSE. The different data formats are: Legacy SOAP/XML, XML, JSON, and Protocol Buffers.

Step 21 Enter the street address of your location in the **Street Address** text box.

Step 22 Enter the phone number where Meridian can reach you for additional information in the **Phone Number** text box.

Step 23 Click **Advanced** to open the Advanced pane.

Step 24 If you want MSE to send real-time notifications to Meridian when ever the wireless clients enter the selected zones, then select the **Enable Zone Notifications for zones** check box and choose floors and zones from the drop-down list.

The **Enable zone notifications for zones** drop-down list shows all the floors and zones that are added to Prime Infrastructure and synced to the MSE.

Step 25 Click **OK** after selecting zones and floors.

Step 26 Click **Save**.

Step 27 Click **Done** to save the MSE settings.

Note The below listed features of MSE are not supported by CMX:

- Managing CMX High Availability
- Synchronization History
- Context Aware Notifications
- Mobile Concierge
- wIPS and Wireless Security
- Location Accuracy

Related Topics

View MSEs, on page 7
Delete MSE License Files, on page 6
Delete MSEs from Prime Infrastructure, on page 7

MSE Licensing

The Cisco MSE provides a wide variety of location-based services. To enable these services, the following are required:

- Cisco MSE hardware or software appliance
  - Physical Appliance—An activation license is not required.
  - Virtual Appliance—Virtual Appliance instance requires an MSE Virtual Appliance Activation license (L-MSE-7.0-K9). It is not sufficient to simply have a service/feature license on an MSE Virtual Appliance.
- Licenses
- Support
- See the chapter *Licenses and Software Updates* in the Cisco Prime Infrastructure Administrator Guide, for more information.

For complete details on ordering and downloading licenses, see the *Cisco Mobility Services Engine Licensing and Ordering Guide* at the following URL : http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

Delete MSE License Files

To delete an MSE license file, follow these steps:

Procedure

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

The Mobility Services page appears.

Step 2 Click **Device Name** to delete a license file for a particular service.

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

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 MSE.

Related Topics

View MSEs, on page 7
Add MSEs to Cisco Prime Infrastructure, on page 2
Delete MSEs from Prime Infrastructure, on page 7
Cisco Prime Infrastructure Data That is Synchronized With MSE, on page 8

View MSEs

To see a list of current Mobility Services, choose **Services** > **Mobility Services** > **Mobility Services Engines**.

The Mobility Services Engines page provides device information and features for each device and a **Select a command** drop-down list.

Location and MSE features of Cisco Prime Infrastructure do not support partitioning.

Related Topics

Add MSEs to Cisco Prime Infrastructure, on page 2
Delete MSE License Files, on page 6
Delete MSEs from Prime Infrastructure, on page 7
Cisco Prime Infrastructure Data That is Synchronized With MSE, on page 8

Delete MSEs from Prime Infrastructure

To delete an MSE from the Prime Infrastructure database, follow these steps:

Procedure

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

The Mobility Services page appears.

Step 2 Select the MSE(s) 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)**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm that you want to delete the selected MSE from the Prime Infrastructure database.

Step 6 Click **Cancel** to stop the deletion.

Related Topics

View MSEs, on page 7
Add MSEs to Cisco Prime Infrastructure, on page 2

Cisco Prime Infrastructure Data That is Synchronized With MSE

This section describes how to synchronize Cisco Prime Infrastructure and MSEs manually and smartly.

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

- Network Designs—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.
- Controllers—A selected controller that is associated and regularly exchanges location information with an MSE. Regular synchronization ensures location accuracy.
- Event Groups—A group of predefined events that define triggers that generate an event. Regular synchronization ensures that the latest defined events are tracked.
- 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 series switches 4000: 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.
- 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 the mobile devices. This shows the service advertisement that has synchronized with the MSE.

Be sure to verify software compatibility between the controller, Cisco Prime Infrastructure, and the MSE before synchronizing.

Communication between the MSE, Cisco Prime Infrastructure, and the controller is in Coordinated Universal Time (UTC). Configuring NTP on each system provides devices with the UTC time. The MSE and its associated controllers must be mapped to the same NTP server and the same Cisco Prime Infrastructure server. An NTP server is required to automatically synchronize time between the controller, Cisco Prime Infrastructure, and the MSE.

Related Topics

View MSEs, on page 7
Synchronize Product Data With MSE, on page 9
Change the MSE Assignment for a Wireless Controller, on page 10
Synchronize Third Party NEs with MSE , on page 11

Set Up Synchronization Between MSE Databases and Product Database, on page 13
View the History of MSE Database and product Database Synchronizations, on page 15

Synchronize Product Data With MSE

To synchronize Prime Infrastructure network designs, controllers, wired switches, or event groups with the MSE, follow these steps:

Procedure

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

Step 2 Choose the appropriate menu option (**Network Designs, Controllers, Event Groups, Wired Switches, Third Party Elements, or Service Advertisements**) from the left sidebar menu.

Step 3 To assign a network design to an MSE, from the left sidebar menu, choose **Network Designs**.

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

Through 6.0, you can assign only up to a campus level to an MSE. Beginning with 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.

A network design might include a floor in a campus or a large campus with several buildings, each monitored by a different MSE. Because of this, you might need to assign a single network design to multiple MSEs.

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

- **Save**—Saves the MSE assignment. The following message appears in the Messages column of the Network Designs page with a yellow arrow icon:

  "To be assigned - Please synchronize”

- **Cancel**—Discards the changes to the MSE assignment and return to the Network Designs page.
- **You can also click Reset** to undo the **MSE** assignments.

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.

Network design assignments also automatically picks up the corresponding controller 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.

You can use the same procedure to assign wired switches or event groups to an MSE.

Related Topics

Cisco Prime Infrastructure Data That is Synchronized With MSE, on page 8
View the History of MSE Database and product Database Synchronizations, on page 15
Change the MSE Assignment for a Wireless Controller, on page 10
Set Up Synchronization Between MSE Databases and Product Database, on page 13

Find and Troubleshoot MSE-Product Out-of-Sync Alarms, on page 28

Change the MSE Assignment for a Wireless Controller

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

To assign an MSE service to wireless controllers, follow these steps:

Procedure

Step 1 In the synchronization page, choose **Controllers**.

Step 2 Choose the controllers to be assigned to the MSE.

Step 3 Click **Change MSE Assignment**.

Step 4 Choose the MSE to which the controllers must be synchronized.

Step 5 Click either of the following in the dialog box:

- **Save**—Saves the **MSE assignment**. The following message appears in the Messages column of the Controllers page:

"To be assigned - Please synchronize".

- **Cancel**—Discards the changes to the MSE assignment and returns to the Controllers page.
- You can also click **Reset** to undo the yellow button assignments.

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

Step 7 Verify that the MSE is communicating with each of the controllers for only the chosen service. This can be done by clicking the **NMSP status** link in the status page. See Troubleshoot NMSP Connection Status, on page 11 for more information.

After Synchronizing a controller, verify that the timezone is set on the associated controller. Controller names must be unique for synchronizing with an MSE. If you have two controllers with the same name, only one is synchronized.

Step 8 If you want to unassign a network design, controller, wired switch, or event group from an MSE, do the following:

a) On the respective tabs, click one or more elements, and click **Change MSE Assignment**. The Choose MSE dialog box appears.
b) Unselect the Mobility Services Engine check box if you do not want the elements to be associated with that MSE.
c) Click **Save** to save the changes to the assignments.
d) Click **Synchronize**. A two-arrow icon appears in the Sync Status column.

Related Topics

Troubleshoot NMSP Connection Status, on page 11
View MSEs, on page 7
Cisco Prime Infrastructure Data That is Synchronized With MSE, on page 8
View the History of MSE Database and product Database Synchronizations, on page 15
Set Up Synchronization Between MSE Databases and Product Database, on page 13

Troubleshoot NMSP Connection Status

If you recently upgraded a controller and NMSP status is inactive on the **Services** > **Mobility Services** > **Synchronize Services** > **Controllers** page, you need to trigger an inventory collection so Prime Infrastructure receives the upgraded controller information:

Procedure

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard**.

Step 2 Select **System Jobs** > **Inventory**, then select **Wireless Controller Inventory**.

Step 3 Click **Run**.

After the job completes, the NMSP Status will be updated.

Related Topics

Change the MSE Assignment for a Wireless Controller, on page 10

Synchronize Third Party NEs with MSE

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

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

Procedure

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

The Network Design page appears.

In the Network Design page, choose **Third Party Elements** from the left sidebar menu.

The Third Party Elements page appears.

Step 2 Select one or more elements.

Step 3 Click one of the following buttons:

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

Related Topics

View MSEs, on page 7
Cisco Prime Infrastructure Data That is Synchronized With MSE, on page 8
View the History of MSE Database and product Database Synchronizations, on page 15
Set Up Synchronization Between MSE Databases and Product Database, on page 13
Change the MSE Assignment for a Wireless Controller, on page 10
Find and Troubleshoot MSE-Product Out-of-Sync Alarms, on page 28

Configure Controller Time Zones to Ensure Proper Synchronization with MSE

For controller Releases 4.2 and later, if an MSE (Release 5.1 or greater) is installed in your network, it is mandatory that the time zone be set on the controller to ensure proper synchronization between the two systems.

Greenwich Mean Time (GMT) is used as the standard for setting the time zone system time of the controller.

You can automatically set the time zone during initial system setup of the controller or manually set it on a controller already installed in your network.

To manually set the time and time zone on an existing controller in your network using the CLI, follow these steps:

Procedure

Step 1 Configure the current local time in GMT on the controller by entering the following commands:

Example:

```
(Cisco Controller) >config time manual 09/07/07 16:00:00
(Cisco Controller) >config end
```

When setting the time, the current local time is entered in terms of GMT and as a value between 00:00 and 24:00. For example, if it is 8 AM Pacific Standard Time (PST) in the US, you enter 16:00 (4 PM PST) as the PST time zone is 8 hours behind GMT.

Step 2 Verify that the current local time is set in terms of GMT by entering the following command:

Example:

```
(Cisco Controller) >show time
Time..................................... Fri Sep 7 16:00:02 2007
Timezone delta........................... 0:0
```

Step 3 Set the local time zone for the system by entering the following commands:

When setting the time zone, you enter the time difference of the local current time zone with respect to GMT (+/-). For example, Pacific Standard Time (PST) in the United States (US) is 8 hours behind GMT (UTC) time. Therefore, it is entered as -8.

Example:

```
(Cisco Controller) >config time timezone -8
(Cisco Controller) >config end
```

Step 4 Verify that the controller shows the current local time with respect to the local time zone rather than in GMT by entering the following command:

Example:

```
(Cisco Controller) >show time
Time..................................... Fri Sep 7 08:00:26 2007
Timezone delta........................... -8:0
```

The time zone delta parameter in the **show time** command shows the difference in time between the local time zone and GMT (8 hours). Before configuration, the parameter setting is 0.0.

Related Topics

View MSEs, on page 7
Cisco Prime Infrastructure Data That is Synchronized With MSE, on page 8
View the History of MSE Database and product Database Synchronizations, on page 15
Set Up Synchronization Between MSE Databases and Product Database, on page 13
Change the MSE Assignment for a Wireless Controller, on page 10
Find and Troubleshoot MSE-Product Out-of-Sync Alarms, on page 28
Synchronize Third Party NEs with MSE , on page 11

Set Up Synchronization Between MSE Databases and Product Database

Manual synchronization of Prime Infrastructure and MSE databases provides immediate synchronization. However, future deployment changes (such as making changes to maps and access point positions), can yield incorrect location calculations and asset tracking until resynchronization reoccurs.

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

Any change to one or more of any synchronized components 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 which is also synchronized with the MSE, then the changed location of the access point is automatically communicated.

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

To configure smart synchronization, follow these steps:

Procedure

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

The Background Tasks summary page appears.

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

Step 3 The Mobility Services Synchronization page appears.

Step 4 To set the MSE to send out-of-sync alerts, select the **Enabled** check box in the Out of Sync Alerts group box.

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

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

When an MSE is added to Prime Infrastructure, the data in 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 Prime Infrastructure are removed automatically from MSE.

Step 6 Enter the time interval, in minutes, that the smart synchronization is to be performed.

By default, smart-sync is disabled.

Step 7 Click **Submit**.

Related Topics

Configure Controller Time Zones to Ensure Proper Synchronization with MSE, on page 12

Examples: How Smart Controllers are Selected When Synchronizing Product Data With MSEs

Scenario 1

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

Scenario 2

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

Scenario 3

An access point is added to a floor and is assigned to an 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 which is synchronized to the MSE are deleted then that controller is automatically removed from MSE assignment or unsynchronized.

Related Topics

Cisco Prime Infrastructure Data That is Synchronized With MSE, on page 8
View the History of MSE Database and product Database Synchronizations, on page 15
Change the MSE Assignment for a Wireless Controller, on page 10
Find and Troubleshoot MSE-Product Out-of-Sync Alarms, on page 28
Synchronize Third Party NEs with MSE , on page 11

View the Status of the MSE Database and product Database Synchronizations

You can use the Synchronize Servers command in Prime Infrastructure to view the status of network design, controller, and event group synchronization with an MSE.

To view synchronization status, follow these steps:

Procedure

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

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

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

A green two-arrow icon does not indicate the NMSP connection status for a controller.

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 MSE the floor is currently assigned to. You can also change MSE assignment from this page.

Related Topics

View MSEs, on page 7
Add MSEs to Cisco Prime Infrastructure, on page 2
Cisco Prime Infrastructure Data That is Synchronized With MSE, on page 8
View the History of MSE Database and product Database Synchronizations, on page 15
Change the MSE Assignment for a Wireless Controller, on page 10
Find and Troubleshoot MSE-Product Out-of-Sync Alarms, on page 28

View the History of MSE Database and product Database Synchronizations

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

The Synchronization History page on the Services tab is available only in the root virtual domain in Release 7.3.

To view synchronization history, choose **Services** > **Synchronization History**, and click the column headers to sort the entries.

Related Topics

View MSEs, on page 7
Synchronize Third Party NEs with MSE , on page 11
Cisco Prime Infrastructure Data That is Synchronized With MSE, on page 8
Change the MSE Assignment for a Wireless Controller, on page 10
Find and Troubleshoot MSE-Product Out-of-Sync Alarms, on page 28
Set Up Synchronization Between MSE Databases and Product Database, on page 13
View the Status of the MSE Database and product Database Synchronizations, on page 14

View the Notification Statistics for an MSE

You can view the notification statistics for a specific MSE. To view the Notification Statistics for a specific MSE:

Choose **Services** > **Mobility Services** > **Mobility Services Engines >** *MSE-name* **Context Aware Service > Notification Statistics** (where *MSE-name* is the name of an MSE).

The following table describes the fields in the Notification statistics page.

Table 1: Notification Statistics fields

Field	Description
Summary	
Destinations	
Total	Total destination count.
Unreachable	Unreachable destination count.
Notification Statistics Summary	
Destination Address	The destination 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 track definition. Track notification status can be either Enabled or Disabled.
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 failed.
Track Definition (Status)	
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.

Change an MSE Server's Basic Properties

You can use Prime Infrastructure to edit the general properties of an MSE registered in Prime Infrastructure database. General properties include contact name, username, password, and HTTP.

To edit the general properties of an MSE, follow these steps:

Procedure

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

Step 2 Click the name of the MSE that you want to edit. The General Properties page (with a General tab and Performance tab) appears.

Step 3 In the General Properties page, modify the following Server Details as necessary:

- Contact Name—Enter a contact name for the mobility service.
- Username—Enter the log in username for the Prime Infrastructure server that manages the mobility service.
- Password—Enter the log in password for the Prime Infrastructure server that manages the mobility service.
- HTTP—Select the **HTTP enable** check box to enable HTTP. When you have a non-default port or HTTPS turned on, you must pass the correct information along with the command. For example, *getserverinfo* must include *-port<<port>> -protocol<<HTTP/HTTPS>>*. Similarly, for stopping the server, *stoplocserver - port <<port>> -protocol <HTTP/HTTPS>>*.
- Legacy Port—8001
- Legacy HTTPS—Select the check box to enable the legacy HTTPS.
- Delete synchronized service assignments and enable synchronization—Select the **Delete synchronized service assignments** 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 an MSE.

Prime Infrastructure always uses HTTPS to communicate with an MSE.

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

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

Step 4 In the Mobility Services dialog box, select the **Admin Status** check box to enable the applicable (Context Aware Service, WIPS, Mobile Concierge Service, Location Analytics Service, Billboard service) service.

If you select Context Aware Service, then you must select a location engine to perform location calculation.

Choose either of the following:

- Cisco Tag Engine

or

- Partner Tag Engine

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

The Mobility Services dialog box also shows the following:

- Service Name

- Service Version
- Service Status
- License Type

Use the **Click here** link to view MSE licensing details.

Step 5 Click **Save** to update Prime Infrastructure and mobility service databases.

Step 6 Click the **Performance** tab to view a graph of CPU and memory utilization percentages.

Change the NMSP Protocol Properties for an MSE

Network Mobility Services Protocol (NMSP) manages communication between the mobility service and the controller. Transport of telemetry, emergency, and RSSI values between the mobility service and the controller is managed by this protocol.

Note The NMSP parameter is supported in mobility services installed with Release 3.0 through 7.0.105.0. It is not supported on releases later than 7.0.105.0.

- NMSP replaces the LOCP term introduced in Release 3.0.
- Telemetry and emergency information is only seen on controllers and Prime Infrastructure installed with Release 4.1 software or greater and on mobility service engine running release 3.0 or later software.
- The TCP port (16113) that the controller and mobility service communicate over must be open (not blocked) on any firewall that exists between the controller and mobility service for NMSP to function.

The NMSP Parameters dialog box inPrime Infrastructure enables you to modify NMSP parameters such as echo and neighbor dead intervals as well as response and retransmit periods.

To configure NMSP parameters, follow these steps:

Procedure

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 From the left sidebar menu, choose **Status** > **NMSP Parameters**.

Step 4 Modify the NMSP parameters as appropriate.

Note We do not recommend you change the default parameter values unless the network is experiencing slow response or excessive latency.

NMSP parameters include the following:

- Echo Interval—Defines how frequently an echo request is sent from a mobility service to a controller. The default value is 15 seconds. Allowed values range from 1 to 120 seconds.
- 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 acknowledgments.
- Neighbor Dead Interval—The number of seconds that the mobility service 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 values is 30 seconds. Allowed values range from 1 to 240 seconds. This value must be at least two times the echo interval value.
- Response Timeout—Indicates how long the mobility service waits before considering the pending request as timed out. The default value is one second. Minimum value is one (1). There is no maximum value.
- Retransmit Interval—Interval of time that the mobility service waits between notification of a response time out and initiation of a request retransmission. The default setting is 3 seconds. Allowed values range from 1 to 120 seconds.
- Maximum Retransmits—Defines the maximum number of retransmits that are done in the absence of a response to any request. The default setting is 5. Allowed minimum value is zero (0). There is no maximum value.

Step 5 Click **Save** to update Prime Infrastructure and mobility service databases.

View MSE Active Sessions

The Active Sessions dialog box in Prime Infrastructure enables you to view active user sessions on the MSE.

Procedure

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

Step 2 Click the name of the MSE.

Step 3 From the left sidebar menu, choose **System** > **Active Sessions**.

Prime Infrastructure shows a list of active mobility service sessions. For every session,Prime Infrastructure shows the following information:

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

View MSE Trap Destinations

The Trap Destinations dialog box of Prime Infrastructuree enables you to specify which Prime Infrastructure or Cisco Security Monitoring, Analysis, and Response System (CS-MARS) network management platform is the recipient of SNMP traps generated by the MSE.

To view a trap destination for an MSE, follow these steps:

Procedure

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

Step 2 Click the name of the MSE.

Step 3 From the left sidebar menu, choose **System** > **Trap Destinations**.

Prime Infrastructure shows a list of current trap destinations including the following information:

- IP address
- Port No.
- Community
- Destination type
- SNMP Version

Use the Select a command drop-down list to add or delete a trap destination.

Related Topics

Configure MSE Trap Destinations, on page 20

Configure MSE Trap Destinations

To add a trap destination, follow these steps:

Procedure

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

Step 2 Click the name of the mobility service.

Step 3 From the left sidebar menu, choose **System** > **Trap Destinations**.

Step 4 Choose **Add Trap Destination** from the command drop-down list and click Go.

The New Trap Destination page appears.

Step 5 Enter the following details (see the following table).

Table 2: Add Trap Destination Page

Field	Description
IP Address	IP address for the trap destination.
Port No.	Port number for the trap destination. The default port number is 162.
Destination Type	This field is not editable and has a value of **Other**.
Snmp Version	Select either v2c or v3.
The following set of fields appear only if you select v3 as the SNMP version.	
User Name	Username for the SNMP Version 3.
Security Name	Security name for the SNMP Version 3.

Field	Description
Authentication Type	Select one of the following: HMAC-MD5 HMAC-SHA
Authentication Password	Authentication password for the SNMP Version 3.
Privacy Type	Select one of the following: CBC-DES CFB-AES-128 CFB-AES-192 CFB-AES-256
Privacy Password	Privacy password for the SNMP Version 3.

Step 6 Click **Save** to save the changes or **Cancel** to discard the changes.

Related Topics

View MSE Trap Destinations, on page 19

Configure Advanced MSE Server Settings

The Advanced Parameters dialog box in Prime Infrastructure enables you to set the number of days events are kept, set session time out values, set an absent data interval cleanup interval, and enable or disable Advanced Debug. You can use Prime Infrastructure to modify troubleshooting parameters for an MSE.

To edit advanced parameters for an MSE, follow these steps:

Procedure

Step 1 Choose **Services** > **Mobility 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
- Advanced Parameters

Caution Because advanced debugging slows the mobility service down, enable advanced debugging only under the guidance of Cisco TAC personnel.

- 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 service hardware. See Reboot an MSE Server, on page 22 for more information.
  - Shutdown Hardware—Click to turn off the mobility service hardware. See Shut Down an MSE Server, on page 22Shut Down an MSE Server the for more information.
  - Clear Database—Click to clear the mobility services database. Unselect the **Retain current service assignments in the** Prime Infrastructure**Prime Infrastructure** check box to remove all existing service assignments from Prime Infrastructure and MSE. The resources have to be reassigned from **Services** > **Synchronize Services** page. This option is selected by default.

Step 5 Click **Save** to update Prime Infrastructure and mobility service databases.

Reboot an MSE Server

If you need to restart an MSE, follow these steps:

Procedure

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

Step 2 Click the name of the MSE that you want to reboot.

Step 3 Click **System**.

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands dialog box, click **Reboot Hardware**.

Step 6 Click **OK** to confirm that you want to reboot the MSE hardware.

The rebooting process takes a few minutes to complete.

Shut Down an MSE Server

If you need to shut down an MSE, follow these steps:

Procedure

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

Step 2 Click the name of the MSE that you want to shut down.

Step 3 Click **System**.

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands dialog box, click **Shutdown Hardware**.

Step 6 Click **OK** to confirm that you want to shut down the MSE.

Restore Factory Settings for the MSE Database (Clear)

To clear an MSE configuration and restore its factory defaults, follow these steps:

Procedure

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

Step 2 Click the name of the MSE you want to configure.

Step 3 Click **System**.

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands dialog box, unselect the **Retain current service assignments in the** Prime Infrastructure**Prime Infrastructure** check box to remove all existing service assignments from Prime Infrastructure and MSE.

The resources have to be reassigned in the **Services >** > **Mobility Services** > **Synchronize Services** page. By default, this option is selected.

Step 6 In the Advanced Commands dialog box, click **Clear Database.**

Step 7 Click **OK** to clear the MSE database.

Configure MSE Logging Levels

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

To configure logging options, follow these steps:

Procedure

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

Step 2 Click the name of the MSE that you want to configure.

Step 3 Choose **System** > **Logs**. The advanced parameters 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 preceding 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 TAC personnel.

Step 5 Select the **Enabled** check box next to each element listed in that section to begin logging its events.

Step 6 Select the **Enable** check box in the Advanced Parameters dialog box to enable advanced debugging. By default, this option is disabled.

Step 7 To download log files from the server, click **Download Logs**. See Download MSE Log Files, on page 24for more information.

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 group box, 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**.

See How MSE MAC Addressed-Based Logging Works How MSE MAC Addressed-Based Logging Works, on page 24 for more information on MAC Address-based logging.

Step 10 Click **Save** to apply your changes.

How MSE MAC Addressed-Based Logging Works

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 might consist of one main and one backup or rollover log file.

The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC Address. The MAC log files that are not updated for more than 24 hours are pruned.

Download MSE Log Files

If you need to analyze MSE log files, you can use Prime Infrastructure to download them to your system. Prime Infrastructure downloads a zip file containing the log files.

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

Procedure

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

Step 2 Click the name of the MSE 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 open the file or save the zip file to your system.

Configure MSE User Accounts

You can configure the MSE User Accounts using the following procedure.

Procedure

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

Step 2 Click the device name of the MSE that you want to edit.

Step 3 From the left sidebar menu, choose **Systems** > **Accounts** > **Users**.

Step 4 If you want to add a user to an MSE, follow these steps:

a) From the **Select a command** drop-down list, choose **Add User**.
b) Click **Go**.
c) Enter the username in the Username text box.
d) Enter a password in the Password text box.
e) Enter the name of the group to which the user belongs in the Group Name text box.
f) Choose a permission level from the Permission drop-down list.
g) There are three permission levels to choose from: Read Access, Write Access, and Full Access (required for Prime Infrastructure to access an MSE).

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

h) Click **Save** to add the new user to the MSE.

Step 5 If you want to delete a user from an MSE, follow these steps:

a) From the left sidebar menu, choose **Systems > Accounts > Users**.
b) Select the check box(es) of the user(s) that you want to delete.
c) From the Select a command drop-down list, choose **Delete User**.
d) Click **Go**.
e) Click **OK** to confirm that you want to delete the selected users.

Step 6 If you want to change user properties, follow these steps:

a) Click the username of the user that you want to edit.
b) Make the required changes to the Password, Group Name, and Permission text boxes.
c) Click **Save** to apply your change.

Configure MSE User Groups to Control Read-Write Access

You can control the Read-Write access of the MSE User group using the following procedure.

Procedure

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

Step 2 Click the device name of the MSE that you want to edit.

Step 3 From the left sidebar menu, choose **Systems** > **Accounts** > **Groups**.

Step 4 If you want to add a user group to an MSE, do the following:

a) From the Select a command drop-down list, choose **Add Group**.
b) Click **Go**.
c) Enter the name of the group in the Group Name text box.
d) Choose a permission level from the Permission drop-down list.

There are three permissions levels to choose from:

- **Read Access**
- **Write Access**
- **Full Access** (required for Prime Infrastructure to access mobility services engines)

e) Click **Save** to add the new group to the MSE.

Caution Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with read access permission, that user cannot configure MSE settings.

Step 5 If you want to delete a user group from an MSE, do the following:

a) Select the check box(es) of the group(s) that you want to delete.
b) From the **Select a command**drop-down list, choose **Delete Group**.
c) Click **Go**.
d) Click **OK** to confirm that you want to delete the selected users.

Step 6 If you want to change user group permissions, do the following:

a) Click the group name of the group that you want to edit.
b) Choose a permission level from the Permission drop-down list.
c) Click **Save** to apply your change.

Caution Group permissions override individual user permissions. For example, if you give a user permission for full access and add that user to a group with read access, that user is unable to configure MSE settings.

Monitor the MSE and Product Servers

The **System > Status** page enables you to monitor server events, Prime Infrastructure alarms and events, and NMSP connection status for the MSE.

To view a list of server events, follow these steps:

Procedure

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

Step 2 Click the name of the applicable MSE.

Step 3 From the left sidebar menu, choose **System** > **Status** > **Server Events**.

The Status > Server Events page provides the following information:

- Timestamp—Time of the server event.
- Severity—Severity of the server event.
- Event—Detailed description of the event.
- Facility—The facility in which the event took place.

View product-related MSE Alarms

You can view the audit logs for User-triggered operations using the Audit Logs option available in an MSE. To view the audit logs, follow these steps:

Procedure

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

Step 2 Click the name of the applicable MSE.

Step 3 From the left sidebar menu, choose **System** > **Status** > **Audit Logs**.

The **Status** > **Audit Logs** page provides the following information:

- Username—The Username which has triggered the audit log.
- Operation—The operation that has been performed by the User.
- Operation Status—The status of the operation and it can be SUCCESSFUL or FAILED.
- Invocation Time—The date and time at which the audit log was recorded for the specified operation.

View MSE Alarms and Events

To view a list of Prime Infrastructure alarms and events, follow these steps:

Procedure

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

Step 2 Click the name of the applicable mobility service.

Step 3 From the left sidebar menu:

- Choose **System** > **Status** > **Prime Infrastructure Alarms**Prime Infrastructure, to view the alarms.
- Choose **System** > **Status** > **Prime Infrastructure Events,** Prime Infrastructure to view the events.

Find and Troubleshoot MSE-Product Out-of-Sync Alarms

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

- Elements have been modified in Cisco Prime Infrastructure (the auto-sync policy pushes these elements).
- Elements have been modified in the MSE.
- Elements except controllers exist in the MSE database but not in Cisco Prime Infrastructure.
- Elements have not been 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

When you delete an MSE, the out-of-sync alarms for that system is also deleted. In addition, if you delete the last available MSE, the alarms for "elements not assigned to any server" are also deleted.

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

By default, out-of-sync alarms are enabled. You can disable them in Cisco Prime Infrastructure by choosing **Administration** > **System Settings** > **Alarms and Events**, and clicking **Mobility Service Synchronization**, unselecting the **Auto Synchronization** check box, and clicking **Submit**.

Monitor the Connection Status Between Controllers and MSEs

The NMSP Connection Status page allows you to verify the NMSP connection between the MSE and the Cisco controller to which the MSE is assigned.

Network Mobility Services Protocol (NMSP) is the protocol that manages communication between the mobility service and the controller.

Procedure

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

Step 2 Click the name of the applicable mobility service.

Step 3 From the left sidebar menu, choose **System** > **Status** > **NMSP Connection Status**.

The NMSP Connection Status page shows the following information:

- Summary—The Summary section shows each device type, the total number of connections, and the number of inactive connections.
- NMSP Connection Status—This group box shows the following:

IP address—Click the device IP address to view NMSP connection status details for this device. See the Monitor the Connection Status Between a Specific Device and MSE, on page 29, for additional information.

- Target Type—Indicates the device to which the NMSP connection is intended.
- Version—Indicates the current software version for the device.
- NMSP Status—Indicates whether the connection is active or inactive.
- Echo Request Count—Indicates the number of echo requests that were sent.
- Echo Response Count—Indicates the number of echo responses that were received.
- Last Message Received—Indicates the date and time of the most recent message received.

Step 4 Verify that the NMSP Status is ACTIVE.

- If active, you can view details on wired switches, controllers, and wired clients.
- If not active, resynchronize Prime Infrastructure device and the MSE.

You can launch an NMSP troubleshooting tool for an inactive connection.

Related Topics

Troubleshoot NMSP Connection Status, on page 11

Monitor the Connection Status Between a Specific Device and MSE

To view NMSP Connection Status details, follow these steps:

Procedure

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

Step 2 Click the name of the applicable mobility service.

Step 3 From the left sidebar menu, choose **System** > **Status** > **NMSP Connection Status**.

Step 4 Click the device IP address to open the NMSP Connection Status Details page. The Details page shows the following information:

- Summary
  - IP Address
  - Version—The current software version for the device.
  - Target Type—The device to which the NMSP connection is intended.
  - NMSP Status—Indicates whether the connection is active or inactive.
  - Echo Request Count—The number of echo requests that were sent.
  - Echo Response Count—The number of echo responses that were received.
  - Last Activity Time—The date and time of the most recent message activity between the device and the MSE.
  - Last Echo Request Message Received At—The date and time the last echo request was received.
  - Last Echo Response Message Received At—The date and time the last echo response was received.
  - Model—The device model.

- MAC Address—The MAC address of the device, if applicable.
- Capable NMSP Services—Indicates the NMSP-capable services for this device such as ATTACHMENT or LOCATION.

- Subscribed Services—Indicates subservices for each subscribed NMSP service. For example, MOBILE_STATION_ATTACHMENT is a subservice of ATTACHMENT.
- Messages
  - Message Type—Message types might include: ATTACHMENT_NOTIFICATION, ATTACHMENT_REQUEST, ATTACHMENT_RESPONSE, CAPABILITY_NOTIFICATION, ECHO_REQUEST, ECHO_RESPONSE, LOCATION_NOTIFICATION, LOCATION_REQUEST, SERVICE_SUBSCRIBE_REQUEST, SERVICE_SUBSCRIBE_RESPONSE.
  - In/Out—Indicates whether the message was an incoming or outgoing message.
  - Count—Indicates the number of incoming or outgoing messages.
  - Last Activity Time—The date and time of the most recent activity or message.
  - Bytes—Size of the message in Bytes.

Configure Settings for MSE Database Backups

To view or edit mobility service backup parameters, follow these steps:

Procedure

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

- Backups located at—Indicates the location of the backup file.
- Enter a name for the Backup—Enter or edit the name of the backup file.
- Timeout (in secs)—Indicates the length of time (in seconds) before attempts to back up files times out.

Back Up MSE Historical Data to the product Server

Prime Infrastructurecontains functionality for backing up MSE data.

Procedure

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

Step 2 Click the name of the MSE that you want to back up.

Step 3 From the left sidebar menu, choose **Maintenance** > **Backup**.

Step 4 Enter the name of the backup.

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

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

Status of the backup can be seen on the page while the backup is in process. Three items are displayed on the page during the backup process: (1) Last Status field provides messages noting the status of the backup; (2) Progress field shows what percentage of the backup is complete; and (3) Started at field shows when the backup began noting date and time.

You can run the backup process in the background while working on other MSE operations in another Prime Infrastructure page.

Backups are stored in the FTP directory that you specify during the Prime Infrastructure installation. However, in the Prime Infrastructure installation, the FTP directory is not specified. It might be necessary to provide the full path of the FTP root.

Restore MSE Historical Data from the Product Server

To restore a file back into the mobility service, follow these steps:

Procedure

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

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

Step 5 Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the MSE.

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

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

Step 7 Click **OK** to confirm that you want to restore the data from the Prime Infrastructure server hard drive.

When the restoration is complete, Prime Infrastructure shows a message to that effect.

You can run the restore process in the background while working on other MSE operations in another Prime Infrastructure page.

Download Software to MSEs

To download software to an MSE using Prime Infrastructure, follow these steps:

Procedure

Step 1 Verify that you can ping the location appliance from Prime Infrastructure or an external FTP server, whichever you are going to use for the application code download.

Step 2 Choose **Services** > **Mobility Services** > **Mobility Services Engines**.

Step 3 Click the name of the MSE to which you want to download software.

Step 4 On the left sidebar menu, choose Maintenance.

Step 5 Click *Download Software* and do one of the following:

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

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

  In the Prime Infrastructure installation, FTP directory is not specified. It might be necessary to give the full path of the FTP root.

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

Step 6 Enter the time, in seconds (between 1 and 1800), after which the software download times out.

Step 7 Click **Download** to send the software to the /opt/installers directory on the MSE.

Configure MSE Partner Systems to Improve Navigation for Mobile Devices (Qualcomm PDS)

The **System** > **Partner Systems** page enables you to do MSE-Qualcomm PDS configuration. This configuration is aimed at providing better navigation capability for the mobile devices. The Partner Discovery Server (PDS) generates encrypted assistance data using the floor plan and AP data which is provided by the MSE. The PDS converts this information into an optimized format that will be used by Qualcomm smart phones.

Configure Qualcomm PDS to Work with MSE

To configure Qualcomm PDS for MSE, follow these steps:

Procedure

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

Step 2 Click the name of the mobility services.

Step 3 From the left sidebar menu, choose **System** > **Partner Systems**.

The Qualcomm PDS Configuration for MSE page appears.

Step 4 If you want o enable MSE-Qualcomm communication, then select the Enable Qualcomm check box.

Step 5 In the Qualcomm PDS Endpoint text box, enter the Qualcomm PDS server URL. This is the URL of the PDS from where you can fetch data assistance. The default URL is http://207.114.133.174:8000/AssistanceDataMgr/AssistanceDataMgrSOAP?wsdl.

Step 6 In the MSE URL to request assistance data text box, enter the MSE URL. This is the URL at which the MSE is accessible by the devices at the venue.

Step 7 In the Cisco Mobile Concierge SSID text box, enter the Mobile Concierge SSID information of the venue to which mobile clients should connect. The Qualcomm smart phones will associate this SSID and communicate with MSE.

Step 8 Enter the venue description in the Venue Description text box.

Step 9 Enter refresh time period for assistance data for MSE in the Refresh time period for assistance data on MSE text box.

Step 10 Enter refresh time period for assistance data for mobile clients in the Refresh time period for assistance data on mobile clients text box.

Step 11 Select the Include Copyright Information check box if the messages/assistance data sent to Qualcomm PDS server and mobile clients should be copyrighted.

Step 12 In the **Copyright Owner** text box, enter the copyright owner information that has to be included.

Step 13 Enter the copyright year to be included in the Copyright Year text box.

Step 14 Click **Save** to save the configuration and Cancel to go back.

How Qualcomm PDS Works with MSE

The MSE-Qualcomm configuration involves the following steps:

- Generate Map Extraction Tool (MET) output from CAD file.
- Input MET Output into Prime Infrastructure.
- Addition of GPS Markers.
- Synchronize the Floor to MSE.
- Provide Qualcomm QUIPS/PDS and Copyright Information.
- On MSE, perform F2 Interface request to Qualcomm PDS server.

Qualcomm's MET is an application that allows you to customize and select various layers from a map file (DXF file) and generates a zip file containing:

- Image file (.PNG format) to be used as floor map on Prime Infrastructure.
- Span.xml file that contains the dimensions of the floor (horizontal and vertical) in meters.
- Qualcomm specific map XML file containing geometric feature information related to walls, doors, points of interest, and so on.

Note MET application is independent of Prime Infrastructure and MSE and can reside an any host machine. Only the output of MET is used as MAP related input information on Prime Infrastructure.

Procedure

Step 1 Start Qualcomm MET tool by following the steps in ReadMe.txt within the MET Tool folder.

Step 2 Input the DXF File in the Map Extraction Tool.

Step 3 Select necessary layers from the left sidebar menu.

Step 4 Save the output of Map Extraction Tool to desired location on the Map Extraction Tool user interface.

Configure the MSE wIPS Service Administrative Settings

The wIPS Service page allows you to view or manage wIPS service administrative settings.

Note Cisco Adaptive wIPS functionality is not supported for non-root partition users.

To view or manage wIPS service administration settings, follow these steps:

Procedure

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

Step 2 Choose the device name of the applicable MSE.

Step 3 From the left sidebar menu, choose **wIPS Service**.

Step 4 View or edit the following parameters:

- Log level—Choose the applicable log level from the drop-down list. Log levels include Debug, Error, Important Event, Major Debug, None, and Warning.
- Forensic size limit (GB)—Enter the maximum allowable size of forensic files.
- Alarm ageout (hours)—Enter the age limit, in hours, for each alarm.
- Device ageout (days)—Enter the age limit, in days, for the device to send alarms.

Step 5 Click **Save** to confirm the changes or **Cancel** to close the page with no changes applied.

Improve Tracking with MSE Context-Aware Service (Location Services)

Context-Aware Service (CAS) software allows an MSE to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location, temperature and asset availability about a client or tag (Cisco CX version or later) from Cisco access points.

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

Mobility services engines do not track or map non-Cisco CX tags.

CAS was previously referred to as Cisco location-based services.

You can modify Context-Aware Service Software properties as to the type and number of clients or tags that are tracked and whether or not locations are calculated for those clients or tags.

You can also modify parameters that affect the location calculation of clients and tags such as Received Signal Strength Indicator (RSSI) measurements.

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

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

Prerequisites for using MSE CAS, Improve Tracking with MSE Context-Aware Service (Location Services)

Before you can use Cisco Prime Infrastructure to view contextual information, initial configuration for the MSE is required using a command-line interface (CLI) console session. See the *Cisco 3355 Mobility Services Engine Getting Started Guide* and the *Cisco 3100 MSE Getting Started Guide* at the following URL: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

Licensing for Clients and Tags

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

- Licenses for tags and clients are offered separately.
- The clients license also contains tracking of rogue clients and rogue access points, and interferers (if enabled).
- Licenses for tags and clients are offered in a variety of quantities, ranging from 1,000 to 12,000 units.

The AeroScout Context-Aware Engine for Tags support 100 permanent tag licenses; Context-Aware Services consists of permanent tag licenses.

Note See the *Release Notes for Cisco 3300 Series Mobility Services Engine for Software Release 6.0* at the following URL: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html for more information on tags and client licenses.

Context-Aware Service General Parameters

To access the Context Aware Service > General page,follow these steps:

Procedure

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

Step 2 Choose **General** from the left sidebar menu.

This page provides the following information:

- Version
- Operational Status
- Number of Tracked Wireless Clients
- Number of Traced Tags
- Number of Tracked Rogue APs
- Number of Tracked Rogue Clients
- Number of Tracked Interferers
- Number of Tracked Wired Clients
- Total Elements Tracked
- Tracked Elements (Wireless Clients, Rogue APs, Rogue Clients, Interferers, and Wired Clients) Limit
- Tracked Tags Limit

Clients represent a snapshot of client count every 15 minutes. **Peak Clients** is the peak count during that15-minute time period. For example, in a 15-minute time period, the client count varies from 100 to 300. When Prime Infrastructure polls MSE, MSE returns the client count as the count at that exact time, which could be any number between 100 to 300, and the Peak Client Count as 300.

Enable and Configure Context-Aware Service Settings on an MSE

The MSE can track up to 25,000 clients or up to 25,000 tags (with the proper license purchase). Updates on the locations of elements being tracked are provided to the MSE from the Cisco wireless LAN controller.

Only those elements designated for tracking by the controller are viewable in Prime Infrastructure maps, queries, and reports. No events and alarms are collected for non-tracked elements and none are used in calculating the 25,000 element limit for clients or tags.

You can modify the following tracking parameters using Prime Infrastructure:

- Enable and disable element locations (client stations, active asset tags, interferers, wired clients, rogue clients, and rogue access points) 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 specific elements you want to track.

For example, given a client license of 12,000 trackable units, you can set a limit to track only 8,000 client stations (leaving 4,000 units available to track 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.

- Disable tracking and reporting of ad hoc rogue clients and access points.

To configure tracking parameters for an MSE, follow these steps:

Procedure

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

Step 2 Click the name of the MSE whose properties you want to edit. The General Properties page appears.

Step 3 Choose **Context-Aware Software > Tracking Parameters** from the Administration subheading to display the configuration options.

Step 4 Modify the following tracking parameters as appropriate (see the following table).

Table 3: Tracking Parameters

Field	Configuration Options
Tracking Parameters	
Wired Clients	**a.** Select the **Enable** check box to enable tracking of client stations by the MSE. In 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. The wired client limiting is supported from MSE 7.0 and Prime Infrastructure 1.0. In other words, you can limit wired clients to a fixed number, say 500. This limit is set to ensure that the licenses are not taken up completely by wired clients and some licenses are available for other devices. **Caution** When upgrading the MSE from 6.0 to 7.0, if any limits have been set on wireless clients or rogues, they reset because of the wired client limit change in 7.0. **Note** Active Value (Display only): Indicates the number of wired client stations currently being tracked. **Note** Not Tracked (Display only): Indicates the number of wired client stations beyond the limit.
Wireless Clients	**a.** Select the **Enable** check box to enable tracking of client stations by the MSE. **b.** Select the **Enable Limiting** check box to set a limit on the number of client stations to track. **c.** Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 25,000 which is the maximum number of clients that can be tracked by an MSE. **Note** The actual number of tracked clients is determined by the license purchased. **Note** Active Value (Display only): Indicates the number of client stations currently being tracked. **Note** Not Tracked (Display only): Indicates the number of client stations beyond the limit.
Rogue Access Points	**a.** Select the **Enable** check box to enable tracking of rogue clients and asset points by the MSE. **b.** Select the **Enable Limiting** check box to set a limit on the number of rogue clients and asset tags stations to track. **c.** Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 25,000 which is the maximum number of rogue clients and access points that can be tracked by an MSE. **Note** The actual number of tracked rogues (clients and access points) is driven by the client license purchased. The user must consider the number of clients that are being tracked in determining the available quantity to allocate to track rogue clients and access points because clients and rogue clients and access points are addressed by the same license. **Note** Active Value (Display only): Indicates the number of rogue clients and access points currently being tracked. **Note** Not Tracked (Display only): Indicates the number of rogue clients and access points beyond the limit.
Exclude Ad-Hoc Rogues	Select the check box to turn off the tracking and reporting of ad hoc rogues in the network. As a result, ad hoc rogues are not displayed on Prime Infrastructure maps or its events and alarms reported.

Field	Configuration Options
Rogue Clients	**a.** Select the **Enable** check box to enable tracking of rogue clients by the MSE. **b.** Select the **Enable Limiting** check box to set a limit on the number of rogue clients to track. **c.** Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 25,000 which is the maximum number of rogue clients that can be tracked by an MSE. **Note** The actual number of tracked rogues (clients and access points) is driven by the client license purchased. The user must consider the number of clients that are being tracked in determining the available quantity to allocate to track rogue clients and access points because clients and rogue clients and access points are addressed by the same license. **Note** Active Value (Display only): Indicates the number of rogue clients being tracked. **Note** Not Tracked (Display only): Indicates the number of rogue clients beyond the limit.
Interferers	**a.** Select the **Enable** check box to enable tracking of the interferers by the MSE. In 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. **Note** Active Value (Display only): Indicates the number of interferers currently being tracked. **Note** Not Tracked (Display only): Indicates the number of interferers beyond the limit.
Asset Tracking Elements	
Active RFID Tags	**a.** Select the **Enable** check box to enable tracking of active RFID tags by the MSE. **Note** The actual number of tracked active RFID tags is determined by the license purchased. **Note** Active Value (Display only): Indicates the number of active RFID tags currently being tracked. It also depends on the tag engine chosen. **Note** Not Tracked (Display only): Indicates the number of active RFID tags beyond the limit.
SNMP Parameters Not applicable to mobility services 7.0.105.0 and later.	
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 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 only.)
SNMP Polling Interval	
Client Stations	Select the **Enable** check box to enable client station polling and enter the polling interval in seconds. Default value is 300. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier only.)

Field	Configuration Options
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 controllers, you must enable the detection of active RFID tags using the **config rfid status enable** CLI command on the controllers.
Rogue Clients and Access Points	Select the **Enable** check box to enable rogue access point polling and enter the polling interval in seconds. Default value is 600. Allowed values are from 1 to 99999.(Configurable in controller Release 4.1 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 only.)

Step 5 Click **Save** to store the new settings in the MSE database.

Customize Which MSE Assets Are Tracked Using Context-Aware Service Filters

You can limit the number of asset tags, wired clients, rogue clients, interferers and access points whose location is tracked by filtering on the following:

- MAC addresses

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

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 as follows:

- Each MAC address should be listed on a single 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 Allowed listing that follows is a wildcard.

Note Allowed MAC address formats are viewable in the Filtering Parameters configuration page. See the following table for details.

EXAMPLE file listing:

[Allowed]00:11:22:33:*22:cd:34:ae:56:4502:23:23:34:*[Disallowed]00:10:*ae:bc:de:ea:45:23

- Probing clients

Probing clients are clients that are associated to another controller but whose probing activity causes them to be seen by another controller and be counted as an element by the “probed” controller as well as its primary controller.

To configure filtering parameters for an MSE, follow these steps:

Procedure

Step 1 Choose **Services** > **Mobility Services** > **Mobility Services Engines**. 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 From the Context-Aware Software menu, choose **Filtering Parameters** from the Administration subheading to display the configuration options.

Step 4 Modify the following filtering parameters as appropriate (see the following table).

Table 4: Filtering Parameters

Field	Configuration Options
Advanced Filtering Parameters	
Duty Cycle Cutoff Interferers	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 Base location license. The default value for the Duty Cycle Cutoff Interferers is 0% and the configurable range is from 0% to 100%. To better utilize the location license, you can choose to specify a filter for interferers based on the duty cycle of the interferer.
MAC Filtering Parameters	
Exclude Probing Clients	Select the check box to prevent location calculation of probing clients.

Field	Configuration Options
Enable Location MAC Filtering	**a.** Select the check box to enable MAC filtering of specific elements by their MAC address. **b.** To import a file of MAC addresses (*Upload a file for Location MAC Filtering* field), browse for the filename and click **Save** to load the file. The imported list of MAC addresses auto-populates the Allowed List and Disallowed List based on their designation in the file. **Note** To view allowed MAC address formats, click the red question mark next to the *Upload a file for Location MAC Filtering* field. **a.** 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. **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 press **Ctrl** to highlight additional MAC addresses. Click **Allow** or **Disallow** based on its desired destination. **Note** If a MAC address is not listed in the Allow or Disallow column, by default, it appears in the Blocked MACs column. If you click the **Unblock** button, the MAC address automatically moves to the Allow column. You can move it to the Disallow column by selecting the Disallow button under the Allow column.

Step 5 Click **Save**to store the new settings in the MSE database.

Configure Settings for Saving Client Stations, Rogue Clients, and Asset Tags Historical Information

You can use Prime Infrastructure to specify how long to store (archive) histories on client stations, rogue clients, and asset tags. These histories are received from those controllers that are associated with the mobility service.

You can also program the mobility service to periodically remove (prune) duplicate data from its historical files to reduce the amount of data stored on its hard drive.

To configure mobility service history settings, follow these steps:

Procedure

Step 1 Choose **Services** > **Mobility 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 **Context Aware Service** > **History Parameters**.

Step 4 Modify the following history parameters as appropriate (see the following table).

Table 5: History Parameters

Field	Description
Archive for	Enter the number of days for the location appliance to retain a history of each enabled category. The default value is 30. Allowed values are from 1 to 99999.
Prune data starting at	Enter the number of hours and minutes at which the location appliance 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 0, which means never, and 99900000). The default start time is 23 hours and 50 minutes, and the default interval is 1440 minutes.
Enable History Logging of Location Transitions for	To enable history logging of Location transitions, choose one or more of the following: • Client Stations • Wired Stations • Asset Tags • Rogue Clients • Rogue Access Points • Interferers **Note** Before the mobility service can collect asset tag data from controllers, you must enable the detection of RFID tags using the **config rfid status enable** CLI command.

Step 5 Click **Save** to store your selections in the location appliance database.

Enable MSE Location Presence to Enhance Location Information

You can enable location presence on the MSE to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by wireless and wired clients on a demand basis 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.

Location Presence can be configured when a new Campus, Building, Floor or Outdoor Area is being added or configured at a later date.

Once enabled, the MSE is capable of providing any requesting Cisco CX v5 client its location.

Note Before enabling this feature, synchronize the MSE.

To enable and configure location presence on an MSE, follow these steps:

Procedure

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

Step 2 Select the MSE to which the campus or building or floor is assigned.

Step 3 From the left sidebar menu, choose **Context Aware Services** > **Administration** > **Presence Parameters**.

Step 4 Select the Service Type **On Demand** check box to enable location presence for Cisco CX clients v5.

Step 5 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 6 Select any or all of the location formats:

a) Select the **Cisco** check box to provide location by campus, building and floor and X and Y coordinates. 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 7 By default, the Location Response Encoding check box is selected. It indicates the format of the information when received by the client. There is no need to change this setting.

Step 8 Select the **Retransmission Rule** check box to allow the receiving client to retransmit the received information to another party.

Step 9 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 10 Click **Save**.

Import and Export MSE Asset, Chokepoint, and TDOA Receiver Information to an MSE

To import asset, chokepoint, and TDOA receiver information for the MSE using Prime Infrastructurefollow these steps:

Procedure

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

Step 2 To import information for an MSE:

a) Click the name of the MSE for which you want to import information.
b) Choose **Context Aware Service > Administration > Import Asset Information**.
c) 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

d) When the import filename is located in the Browse text box, click **Import**.

Step 3 To export asset, chokepoint, and TDOA receiver information from the MSE to a file using Prime Infrastructure:

a) Click the name of the MSE from which you want the export information.
b) Choose **Context Aware Services** > **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

c) Click **Export**.

   Click **Open** (display to screen), **Save (to external PC or server),** or **Cancel** (to cancel the request).

   If you select **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 the download is complete.

Import Civic Address Information to an MSE

To import civic information for the MSE using Prime Infrastructure, follow these steps:

Procedure

Step 1 Choose **Services** > **Mobility Services** > **Mobility Services Engines**.
Step 2 Click the name of the MSE for which you want to import asset information.
Step 3 From the left sidebar menu, choose **Context Aware Software**.
Step 4 From the Administration left sidebar menu, choose **Import Civic Information**.
Step 5 Enter the name of the text file or browse for the filename.

Information in the imported file should be one of the following formats:

Switch IP Address, Slot Number, Port Number, Extended Parent Civic Address, X, Y, Floor ID, Building ID, Network Design ID, ELIN:”ELIN”, PIDF-Lo-Tag:”Civic Address Element Value”

Each entry must appear on a separate line.

Step 6 Click **Import**.

View Details About the Wired Switches and Clients That Are Synchronized with an MSE

This section describes the **Context Aware Service > Wired** drop-down list parameters.

View Wired Switches That Are Synchronized with an MSE (CAS)

You can review details on the wired switch (IP address, MAC address, serial number, software version, and ELIN), its port, its wired clients (count and status), and its civic information.

Wired switch data is downloaded to the MSE through Prime Infrastructure when the Ethernet switch and the MSE are synchronized (Services > Synchronize Services > Switches). Communication between a location-capable switch and the MSE is over NMSP. Prime Infrastructure and the MSE communicate over XML.

To view details on wired switches, follow these steps:

Procedure

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

Step 2 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 Click the IP address link for the applicable wired switch. The Wired Switch Details page appears.

The Wired Switch Details page has four tabs: Switch Information, Switch Ports, Civic, and Advanced.

You can export civic information from the switch by choosing that option from the Select a command drop-down list. This option is available in all four dashlets of the Wired Switches page.

The Wired Switch Details tabs shows the following information:

- Switch Information—Displays a total count summary of wired clients connected to the switch along with the state of the client (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 in one of the client count links (total clients, connected, disconnected, and unknown). See View Wired Clients That Are Synchronized with an MSE (CAS), on page 46 for more information.

- Switch Ports—Displays 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, port type, and port number by clicking in the respective column heading.

- Civic—Displays a detailed list of the civic information for the wired switch.
- Advanced—Displays a detailed list of the additional civic information for the wired switch.

View Wired Clients That Are Synchronized with an MSE (CAS)

You can view details on a wired client (MAC address, IP address, username, serial number, UDI, model no., software version, VLAN ID, and VLAN ID), port association, and its civic information.

Wired client data is downloaded to the MSE through Cisco Prime Infrastructure when the switch and the MSE are synchronized (Services > Synchronize Services > Switches).

Cisco Prime Infrastructure and the MSE communicate over XML.

You can view the details of the wired client on 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 field on the wired clients page.
- If you want to examine wired clients as they relates to a specific switch, you can view that information on the wired switches page. See View Wired Switches That Are Synchronized with an MSE (CAS), on page 45 for more information.

To view details on a wired client, follow these steps:

Procedure

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

Step 2 Click the device name link of the appropriate MSE.

Step 3 Choose **Context Aware Service** > **Wired** > **Wired Clients**.

In the Wired Clients summary page, clients are grouped by their switch.

A client status is noted as connected, disconnected, or unknown:

- 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. See Monitor the Connection Status Between Controllers and MSEs, on page 28 for more information about NMSP connections.

If you know the MAC address of the wired client, you can click that link to reach the detail page of the client or use the search field.

You can also search for a wired client by its IP address, username, or VLAN ID.

If you click the IP address of the switch, you are forwarded to the detail page of the switch. See View Wired Switches That Are Synchronized with an MSE (CAS), on page 45 for more information.

Step 4 Click the MAC address link for the applicable wired client. The Wired Client Details page appears.

The Wired Client Details page has four tabs: Device Information, Port Association, Civic Address, and Advanced.

The Wired Switch Details tabs show the following information:

- Device Information—Display MAC and IP address, username, serial and model number, UDI, software version, VLAN ID, and VLAN name.

- Port Association—Displays 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.
- Civic Address—Displays any civic address information.
- Advanced—Displays extended physical address details for the wired clients, if applicable.

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 is defined for the its port (port/slot/module) then no location data is displayed.

Configure MSE CAS to Send Tag Notifications to Third-Party (Northbound) Applications

Northbound notifications define which tag notifications the MSE sends to third-party applications.

To configure northbound parameters, follow these steps:

Procedure

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

Step 2 Click the name of the MSE 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 Notification Contents check boxes.

Step 7 Select the **Notification Triggers** check box.

Step 8 Select one or more of the Notification Triggers check boxes.

Step 9 Enter the IP address or hostname and port for the system that is to receive the northbound notifications.

Step 10 Choose the transport type from the drop-down list.

Step 11 Select the **HTTPS** check box if you want to use HTTPS protocol for secure access to the destination system.

Step 12 To modify the notification parameter settings, enter the new value in the appropriate text box in the Advanced tab of this page. See the following table.

Table 6: User-Configurable Conditional and Northbound Notifications Fields

Field	Configuration Options
Rate Limit	Enter the rate, in milliseconds, at which the MSE generates notifications. A value of 0 (default) means that the MSE generates notifications as fast as possible (Northbound notifications only).
Queue Limit	Enter the event queue limit for sending notifications. The MSE drops any event above this limit.
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 MSE does not store events in its database.

Field	Configuration Options
Refresh Time	Enter the wait time in minutes that must pass before a notification is resent. For example, if a device is configured for In Coverage Area notification and it is constantly being detected within the Coverage Area. The notification is sent once every refresh time. Default value is 0 minutes.
Drop Oldest Entry on Queue Overflow	(Read-only). The number of event notifications dropped from the queue since startup.
Serialize Events per Mac address per Destination	Select this option if you want the successive events for the same MAC address to be sent to a single destination in a serial manner.

Step 13 Click **Save**.

Set MSE CAS Location Parameters

You can use Prime Infrastructure to specify whether the mobility service retains its calculation times and how soon the mobility service deletes its collected Received Signal Strength Indicator (RSSI) measurement times. You can also apply varying smoothing rates to manage location movement of an element.

To configure location parameters, follow these steps:

Procedure

Step 1 Choose **Services** > **Mobility 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 **Context Aware Service** > **Location Parameters**.
Step 4 Modify the location parameters as appropriate (See *Cisco Prime Infrastructure 3.2 Reference Guide*).
Step 5 Click **Save** to store your selections in Prime Infrastructure and mobility service databases.

Set MSE CAS Event Notifications

You can use Prime Infrastructure to configure MSE event notification parameters that define such items as how often the notifications are generated or resent by the MSE.

Modify notification parameters only if you expect the MSE to send a large number of notifications or if notifications are not being received.

You can also enable forwarding of northbound notifications for tags to be sent to third-party applications.

The format of northbound notifications sent by the MSE is available on the Cisco developers support portal at the following URL:

http://www.cisco.com/en/US/products/svcs/ps3034/ps5408/ps5418/serv_home.html

To configure notification parameters, follow these steps:

Procedure

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

Step 2 Click the name of the MSE you want to configure.

Step 3 From the Context Aware Software left sidebar menu, choose **Notification Parameters** from the Advanced sub-heading 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 Notification content options.

Step 7 Select the **Notification Triggers** check box.

Step 8 Select one or more of the Notification trigger options.

Step 9 Enter the IP address 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 **HTTPS** if you want to use HTTPS protocol for secure access to the destination system.

Step 12 To modify the notification parameter settings, enter the new value in the appropriate text box in the Advanced tab of the page. (See *Cisco Prime Infrastructure 3.2 Reference Guide*).

Step 13 Click **Save**.

View Context Aware Partner and Tag Engine Status for MSE

To access the Partner Engine Status page, choose **Services** > **Mobility Services** > **Mobility Services Engines** > *MSE Name* > **Context Aware Service** > **Partner Engine** > **Status**.

If tag licenses are available, then Aeroscout Tag Engine is enabled. Otherwise, Cisco Partner Engine is enabled by default.

If only the evaluation license is available, then the Cisco Partner Engine is enabled by default. The Partner Engine status page shows status based on whether it is a Aeroscout Tag Engine or Cisco Tag Engine. See *Cisco Prime Infrastructure 3.2 Reference Guide*.

Note The Aeroscout engine fails to start on MSE if the Cisco Prime Infrastructure map names have special characters such as '&'.

View the Notifications Sent By an MSE (CAS)

To view the Notification Summary, choose **Services** > **Mobility Services** > **Context Aware Service** > **Notifications Summary**.

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

- Absence (Missing)—Generated when the mobility service cannot see the asset in the WLAN for the specified time.

- Location Change Events—Generated when client stations, asset tags, rogue clients, and rogue access points move from their previous location.
- Chokepoint Notifications—Generated when a tag is seen (stimulated) by a chokepoint. This information is only reported and displayed for CCX v.1-compliant tags.
- Battery Level—Generated when a tracked asset tag hits the designated battery level.
- In/Out Area—Generated when an asset is moved inside or outside a designated area.

You define a containment area (campus, building, or floor) in the Maps section of Cisco Prime Infrastructure. You can define a coverage area using the Map Editor.

- Movement from Marker—Generated when an asset is moved beyond a specified distance from a designated marker you define on a map.
- Emergency—Generated for a CCX v.1 compliant asset tag when the panic button of the tag is triggered or the tag becomes detached, tampered with, goes inactive or reports an unknown state. This information is only reported and displayed for CCX v.1 compliant tags.

The summary details include the following:

- All Notifications
- Client Stations
- Asset Tags
- Rogue Clients
- Rogue Access Points

To view details for each of the notifications, click the number under the Last Hour, Last 24 Hours, or Total Active column to open the details page for the applicable notification.

How MSE Notifications are Cleared (CAS)

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

- Missing (Absence)—Elements reappear.
- In/Out Area (Containment)—Elements move back in or out of the containment area.
- Distance—Elements move back within the specified distance from a marker.
- Location Changes—Clear state is not applicable to this condition.
- Battery Level—Tags are detected again operating with Normal battery level.
- Emergency
- Chokepoint

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

View the Current Definitions for MSE Notifications (CAS)

To view the Notification Definitions, choose **Services** > **Mobility Services** > **Context Aware Notifications** > **Notifications Definition**. You can add event groups and event definitions to a group in this page. Every groups help you organize your event notifications. An event definition must belong to a particular group.

For more information on adding event groups and event definitions, see Configure Event Groups for MSE Notifications, on page 53 and Add an MSE Event Definition to an Event Group, on page 56.

The Notification Definition page displays the following parameters only after adding event groups and event definitions:

The following table lists and describes the fields in the Notification Definition page.

Table 7: Notification Definition Page

Field	Description
Group Name	Name of the group to which the event definition is added.
Event Definitions	Existing event definitions for the event group.
Created On	Date on which the event groups are created.

View the Notification Statistics for a Specific MSE (CAS)

You can view the notification statistics for a specific MSE. To view the Notification Statistics for a specific MSE, choose **Services** > **Mobility Services** > *MSE-name* > **Context Aware Service** > **Notification Statistics** (where *MSE-name* is the name of an MSE).

The following table lists and describes the fields in the Notification statistics page.

Table 8: Notification Statistics Fields

Field	Description
Summary	
Destinations	
Total	Total count of the destinations.
Unreachable	Count of unreachable destinations.
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 Northbound 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. For 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.

View MSE Mobile Concierge Advertisements

To view the configured service advertisements, follow these steps:

Procedure

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

Step 2 Click **Device Name** to view its properties.

Step 3 Choose **Mobile Concierge Service** > **Advertisements** from the left sidebar menu.

The following information appears in the Mobile Concierge Service page:

- Icon—Displays an icon associated with the service provider.
- Provide Name—Displays the service providers name.
- Venue Name—Displays the venue name.
- Advertisements
  - Friendly Name—Friendly name that is displayed in the handset.
  - Advertisement Type—Type of advertisement that is displayed in the handset.

View MSE Mobile Concierge Statistics

To view Mobile Concierge service statistics, follow these steps:

Procedure

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

Step 2 Click **Device Name** to view its properties.

Step 3 Choose Mobile **Concierge service** > **Statistics** from the left sidebar menu.

The following information appears in the **Mobile Concierge Service** page:

- Top 5 Active Mobile MAC addresses—Displays information of the most active mobiles in a given venue.
- Top 5 Service URIs—Displays information of the usage of the services across a given venue or provider.

What are MSE Event Groups?

To manage events more efficiently, you can use Cisco Prime Infrastructure to create event groups. Event groups help you organize your event definitions.

Configure Event Groups for MSE Notifications

To add an event group, follow these steps:

Procedure

Step 1 Choose **Services** > **Mobility Services** > **Context Aware Notifications**.
Step 2 Choose **Notification Definitions** from the left sidebar menu.
Step 3 From the Select a command drop-down list, choose **Add Event Group**.
Step 4 Click **Go**.
Step 5 Enter the name of the group in the Group Name text box.
Step 6 Click **Save**.

The new event group appears in the Event Settings page.

Delete Event Groups for MSE Notifications

To delete an event group, follow these steps:

Procedure

Step 1 Choose **Services** > **Mobility Services** > **Context Aware Notifications**.
Step 2 Choose **Notification Definitions** from the left sidebar menu.
Step 3 Select the check box of the event group you want to delete.
Step 4 From the Select a command drop-down list, choose **Delete Event Group(s)**.
Step 5 Click **Go**.
Step 6 Click **OK** to confirm the deletion.
Step 7 Click **Save**.

Configure New MSE Events (Event Definitions)

An event definition contains information about the condition that caused the event, the assets to which the event applies, and the event notification destinations. This section describes how to add, delete, and test event definitions.

Prime Infrastructure enables you to add definitions on a per-group basis. Any new event definition must belong to a particular group.

To add an event definition, follow these steps:

Procedure

Step 1 Choose **Services** > **Mobility 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 the event. An event definition summary page appears for the selected event group.

Step 4 From the Select a command drop-down list, choose **Add Event Definition**.

Step 5 Click **Go**.

Step 6 Enter the name of the event definition in the Event Definition Name text box.

The event definition name must be unique within the event group.

Step 7 Click **Save**.

Step 8 On the General tab, manage the following parameters:

- Admin Status—Enable event generation by selecting the **Enabled** check box (disabled by default).
- Priority—Set the event priority by choosing a number from the drop-down list. Zero is highest.
- An event definition with higher priority is serviced before event definitions with lower priority.
- Activate—To continuously report events, choose the **All the Time** check box. To indicate specific days and times for activation, unselect the **All the Time** check box and choose the applicable days and From/Until times. Click **Save**.

Step 9 On the Conditions tab, add one or more conditions. For each condition, specify the rules for triggering event notification. To add a condition, follow these steps:

a) Click **Add** to open the Add/Edit Condition page.

b) Choose a condition type from the Condition Type drop-down list and configure its associated Trigger If parameters see (See the following table).

Table 9: Condition Type/Trigger If Parameters

Condition Type	Trigger If
Missing	Missing for Time (mins)—Enter the number of minutes after which a missing asset event is generated. For example, if you enter 10 in this text box, the MSE generates a missing asset event if the MSE has not located the asset for more than 10 minutes.
In/Out	Inside of or Outside of—Click **Select Area** and choose the area parameters from the Select page. 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).
Distance	In the distance of *x* (feet) from Marker text box—Enter the distance in feet that triggers an event notification if the monitored asset moves beyond the specified distance from a designated marker. Click **Select Marker** and choose the marker parameters in the Select page. Click **Select**.
Battery Level	Battery Level Is—Low, Medium, Normal. Select the appropriate battery level that triggers an event.
Location Change	An event is triggered if the location of the asset changes.
Emergency	Select **Any**, **Panic Button**, **Tampered**, or **Detached check box.**

Condition Type	Trigger If
Chokepoint	In the range of Chokepoints—Click **Select Chokepoint** check box and choose the chokepoint parameters in the Select page. Click **Select**.

c) In the Apply To drop-down list, choose the type of asset (Any, Clients, Tags, Rogue APs, Rogue Clients or Interferers) for which an event is generated if the trigger condition is met.
d) Emergency and chokepoint events are only applicable to tags (CCXv.1 compliant).
e) From the Match By drop-down list, choose the matching criteria (MAC Address, Asset Name, Asset Group, or Asset Category), the operator (Equals or Like), and enter the relevant text for the selected Match By element.
f) Click **Add**.

Step 10 On the Destination and Transport tab, follow these steps to add one or more destinations to receive event notifications and configure the transport settings:

a) Click **Add** to open the Add/Edit Destination and Transport page.
b) To add one or more new destinations, click **Add New**, enter the applicable IP address, and click **OK**.
c) The recipient system must have an event listener running to process notifications. By default, when you create an event definition, Prime Infrastructure adds its IP address as the destination.
d) To select a destination to receive notifications, click to highlight one or more IP addresses in the box on the right and click **Select** to add the IP address(es) to the box on the left.
e) From the Message Format field drop-down list, select **XML** or **Plain Text**.
f) If you select Prime Infrastructure as the destination, you must select XML format.
g) Choose one of the following transport types from the Transport Type drop-down list:

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

h) Click **Add**.

Add an MSE Event Definition to an Event Group

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

Prime Infrastructure enables you to add definitions for each group. An event definition must belong to a group. See the Cisco Content-Aware Software Configuration Guide for more information on deleting or testing event definitions.

To add an event definition, follow these steps:

Procedure

Step 1 Choose **Services** > **Mobility Services** > **Context Aware Notifications**.

Step 2 Choose **Notification Definitions** from the left sidebar menu.

Step 3 Click the name of the group to which you want to add to the event. An event definition summary page appears for the selected event group.

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

Step 5 On the Conditions tab, add one or more conditions. For each condition you add, specify the rules for triggering event notifications.

Tip For example, to keep track of heart monitors in a hospital, you can add rules to generate event notifications when a heart monitor is missing for one hour, a heart monitor moves off its assigned floor, or a heart monitor enters a specific coverage area within a floor.

To add a condition, follow these steps:

a) Click **Add** to add a condition that triggers this event.

b) In the Add/Edit Condition dialog box, follow these steps:

1. Choose a condition type from the Condition Type drop-down list.

   If you chose Missing from the Condition Type drop-down list, enter the number of minutes after which a missing asset event is generated. For example, if you enter 10 in this text box, the mobility service engine generates a missing asset event if the mobility service engine has not found the asset for more than 10 minutes. Proceed to Step c.

   If you chose In/Out from the Condition Type drop-down list, choose **Inside of** or **Outside of**, then select **Select Area** to select the area to monitor for assets going into it or out of it. 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 c.

   If you chose Distance from the Condition Type drop-down list, enter the distance in feet that triggers an event notification if the monitored asset moves beyond the specified distance from a designated marker, then click **Select Marker**. In the Select dialog box, choose the campus, building, floor, and marker from the corresponding drop-down list, and click **Select**. For example, if you add a marker to a floor plan and set the distance in the Trigger. If the text box is set to 60 feet, an event notification is generated if the monitored asset moves more than 60 feet away from the marker. Proceed to Step c.

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 battery level (low, medium, normal) that triggers an event. Proceed to Step c.

If you chose Location Change from the Condition Type drop-down list, proceed to Step c.

If you chose Emergency from the Condition Type drop-down list, click the button next to the emergency (any, panic button, tampered, detached) that triggers an event. Proceed to Step c.

If you chose Chokepoint from the Condition Type drop-down list, proceed to Step c. There is only one trigger condition, and it is displayed by default. No configuration is required.

c) From the Apply To drop-down list, choose the type of asset (Any, Clients, Tags, Rogue APs, Rogue Clients, or Interferers) for which an event is generated if the trigger condition is met.

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

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

d) From the Match By drop-down list, choose the matching criteria (MAC Address, Asset Name, Asset Group, or Asset Category), the operator (Equals or Like) from the drop-down list, and enter the relevant text for the selected Match By element.

Some examples of asset matching criteria that you can specify:

- If you choose **MAC Address** from the Match By drop-down list, choose **Equals** from the Operator drop-down list, and enter a MAC address (for example, 12:12:12:12:12:12), 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 Match By drop-down list, choose **Like** from the Operator drop-down list, and enter **12:12**, the event condition applies to elements whose MAC address starts with 12:12.

e) Click **Add** to add the condition you have just defined.

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

To select a chokepoint, do the following:

1. Click **Select Chokepoint**. An entry page appears.
2. Choose **Campus**, **Building**, and **Floor** from the appropriate drop-down lists.
3. Choose a Chokepoint from the menu that appears.

You are returned to the Add/Edit Condition page, and the location path (Campus > Building > Floor) for the chokepoint auto-populates the text area next to the Select Checkpoint button.

Step 6 On the Destination and Transport tab, follow these steps to add one or more destinations to receive event notifications and to configure the transport settings:

a) To add a new destination, click **Add**. The Add/Edit Destination configuration page appears.
b) Click **Add New**.
c) Enter the IP address of the system that receives event notifications, and click **OK**.
d) The recipient system must have an event listener running to process notifications. By default, when you create an event definition,Cisco Prime Infrastructure adds its IP address as the destination.
e) To select a destination to send event notifications to, highlight one or more IP addresses in the box on the right, and click **Select** to add the IP addresses to the box on the left.

f) Choose **XML** or **Plain Text** to specify the message format.

g) Choose one of the following transport types from the Transport Type drop-down list:

- SOAP—Specifies Simple Object Access Protocol, a simple XML protocol, as the transport type for sending event notifications. Use SOAP to send notifications over HTTP/HTTPS that are processed by web services on the destination.
- If you choose SOAP, specify whether to send notifications over HTTPS by selecting its corresponding check box. If you do not, HTTP is used. Also, enter the destination port number in the Port Number text box.
- Mail—Use this option to send notifications through e-mail.
- If you choose Mail, you need to choose the protocol for sending the e-mail from the Mail Type drop-down list. You also need to enter the following information: username and password (if Authentication is enabled), name of the sender, prefix to add to the subject line, e-mail address of recipient, and a port number if necessary.
- SNMP—Use Simple Network Management Protocol, a very common technology for network monitoring used to send notifications to SNMP-capable devices.
- If you choose SNMP, enter the SNMP community string in the SNMP Community text box and the port number to send notifications to in the Port Number text box.
- SysLog—Specifies the system log on the destination system as the recipient of event notifications.
- If you choose SysLog, enter the notification priority in the Priority text box, the name of the facility in the Facility text box, and the port number of the destination system in the Port Number text box.

h) To enable HTTPS, select the **Enable** check box next to it.

Port Number auto-populates.

i) Click **Save**.

Step 7 On the General tab, follow these steps:

a) Select the **Enabled** check box for Admin Status to enable event generation (disabled by default).
b) Set the event priority by choosing a number from the **Priority** drop-down list. Zero is the highest priority.
c) An event notification with high priority is serviced before event definitions with lower priority.
d) To select how often the event notifications are sent:
e) Select the **All the Time** check box to continuously report events. Proceed to Step g.
f) Unselect the **All the Time** check box to select the day and time of the week that you want event notifications sent. Days of the week and time fields appear for the selection. Proceed to Step d.
g) Select the check box next to each day you want the event notifications sent.
h) Select the time for starting the event notification by selecting the appropriate hour, minute, and AM/PM options from the Apply From heading.
i) Select the time for ending the event notification by selecting the appropriate hour, minute, and AM/PM options from the Apply Until heading.
j) Click **Save**.

Step 8 Verify that the new event notification is listed for the event group (Mobility > Notifications > Settings > Event Group Name).

Delete Event Definitions for MSE Notifications

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

Procedure

Step 1 Choose **Services > Mobility Services > Context Aware Notifications**.
Step 2 From the left sidebar menu, choose **Settings**.
Step 3 Click the name of the group from which you want to delete the event definitions.
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)**.
Step 6 Click **Go**.
Step 7 Click **OK** to confirm that you want to delete the selected event definitions.

Search for Specific MSE Wireless Clients (IPv6)

Note Only wireless clients have IPv6 addresses in this release.

To search for an MSE located clients using the Prime Infrastructure Advanced search feature, follow these steps:

Procedure

Step 1 Click **Advanced Search**.
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**.

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**.

Searching a client by IP address can contain either 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 as MSE.

This displays clients located by Context-Aware Service in the MSE by directly communicating with the controllers.

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.

If you are searching for the client from Prime Infrastructure on the MSE by IPv4 address, enter the IPv4 address in the Client IP address text box.

Step 9 From the Client States drop-down list, choose the client states. The possible values for wireless clients are **All States**, **Idle**, **Authenticated**, **Associated**, **Probing**, or **Excused**. The possible values for wired clients are **All States**, **Authenticated**, and **Associated**.

Step 10 From the Posture Status drop-down list, choose the posture status to know if the devices are clean or not. The possible values are **All**, **unknown**, **Passed**, **and Failed**.

Step 11 Select the **CCX Compatible** check box to search for clients that are compatible with Cisco Client Extensions. The possible values are **All Versions**, **V1**, **V2**, **V3**, **V4**, **V5**, and **V6**.

Step 12 Select the **E2E Compatible** check box to search for clients that are end-to-end compatible. The possible values are **All Versions**, **V1**, and **V2**.

Step 13 Select the **NAC State** check box to search for clients identified by a certain Network Admission Control (NAC) state. The possible values are **Quarantine**, **Access**, **Invalid**, and **Not Applicable**.

Step 14 Select the **Include Disassociated** check box to include clients that are no longer on the network but for which 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.

View All MSE Clients

You can see the clients in probing state on 2.4 GHz on Cisco WLC but in probing state only on “a” radio (in the **Monitor > Clients and Users > Client detected by MSE** page). None of the clients shows up in probing state on “b/g” radio. This is because when clients are in the probing state, Prime Infrastructure does not get details on the protocol and by default these are shown to be on 5 GHz channel. After they are associated, the INFO messages are received from the controller which contain details on the protocol and the channel. But when they are probing with Measurement messages, Prime Infrastructure does not have this information and defaults it to 5 GHz.

To view all the clients detected by the MSE, follow these steps:

Procedure

Step 1 Choose **Monitor > Monitoring Tools > Clients and Users** to view both wired and wireless clients information.

The Clients and Users table displays a few column by default. If you want to display the additional columns that are available, click 330159 image, and then click **Columns**. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.

Step 2 Filter the current list to choose all the clients that are detected by the MSE by choosing **Clients detected by MSE** from the Show drop-down list.

All the clients detected by MSE including wired and wireless appear.

See Cisco Prime Infrastructure 3.2 Reference Guide, for the details of different parameters are available in the Clients Detected by MSE table.

Step 3 Select the radio button next to MAC Address in the Client and User page to view the associated client information.

Step 4 If you want to access the alarm details for a particular MSE, do the following:

a) Choose **Monitor > Monitoring Tools > Alarms and Events**, and click an MSE item under **Failure Source** column.

or

b) Choose **Services** > **Mobility Services Engines**> *MSE Name* > **System** > **Status** > **Prime Infrastructure Alarms**, and click a particular MSE item under Failure Source column.

See Cisco Prime Infrastructure 3.2 Reference Guide, for the descriptions of fields in the Alarm Detail page.

Configure Mobile Concierge Using MSE

The Mobile Concierge service allows the venue owners and service providers to monitor their WLAN. This solution delivers a unique in-store experience to customers who are using smart phones.

Mobile Concierge service uses wireless smart phones that have been configured with a set of policies for establishing network connectivity. Mobile Concierge service facilitates smartphones to discover network-based services available. Once you are connected to the stores Wi-Fi network, you can join the stores wireless guest network and can access variety of different services including electronic coupons, promotional offers, customer loyalty data, product suggestions, allow you to organize shopping lists, receive unique digital signature based on shopping preferences.

Related Topics

Configure Venues for Mobile Concierge (MSE), on page 61
Configure Providers for Mobile Concierge (MSE), on page 63
Configure Mobile Concierge Policies (MSE), on page 63

Configure Venues for Mobile Concierge (MSE)

To define a venue, follow these steps:

Procedure

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

Step 2 Choose **Mobile Concierge Services > Venues** from the left sidebar menu.

The Venues 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, you can configure the following:

- From the **Area Type** drop-down list, choose the area type where you want to display the service advertisement. The possible values are Floor Area and Outdoor Area.

Note The Building, Floor Area, and**Coverage Area** drop-down lists are displayed only if 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 From the **Audio** group box, click Choose File to browse and select the audio file to play the audio notification.

Step 8 Click **Next**. The Icons group box appears.

Step 9 From the **Icons** group box, click **Choose File** to browse and select the icon that you want to display on the clients handset.

Step 10 Click **Next**. The Venue Apps group box appears.

Step 11 From the Venue **Apps** group box, choose the venue app on which you want to display the service advertisement from the Web App drop-down list.

Step 12 Click **Next**. The **Additional Venue Information** group box appears.

Step 13 From the **Additional Information** group box, you can provide any additional information that the venue would like to provide to the mobile application. You can configure the following:

- Enter the location detail in the **Location Detail** text box. This provides 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 the venue would like to provide to the mobile application in the **Additional Information** text box.

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

Step 15 If you want to delete any venue, do the following in the Venue page:

a) Select the check box of the venue that you want to delete.
b) From the **Select a command** drop-down list, choose **Delete Venue**, and click **Go**.
c) Click **OK** to confirm the deletion.

Related Topics

Configure Mobile Concierge Using MSE, on page 61
Configure Providers for Mobile Concierge (MSE), on page 63
Configure Mobile Concierge Policies (MSE), on page 63

Configure Providers for Mobile Concierge (MSE)

Procedure

Step 1 Choose **Services** > **Mobility Services** > **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 providers venue name in the **Provider Name** text box.

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

Step 6 From the **Icons** group box, click **Choose File** to browse and select the icon that you want to display on the clients handset.

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

Step 8 From the **Local Services** group box, do the following:

- Click the 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 display name in the **Display Name** text box.
  - Enter the description in the **Description** text box.
  - Choose the service URIs from the **Service URIs** drop-down list.
  - Enter the recommended application for the venue in the **Recommended Apps** text box.

Step 9 Click **Save**.

Step 10 If you want to delete a provider, do the following in the Providers page:

a) Select the check box of the venue that you want to delete.
b) From the **Select a command** drop-down list, choose **Delete Provider**, and click **Go**.
c) Click **OK** to confirm the deletion.

Related Topics

Configure Venues for Mobile Concierge (MSE), on page 61
Configure Mobile Concierge Using MSE, on page 61
Configure Mobile Concierge Policies (MSE), on page 63

Configure Mobile Concierge Policies (MSE)

To configure policies, follow these steps:

Procedure

Step 1 Choose **Services** > **Mobility 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 provider from the **Provider** drop-down list.

Step 7 Click **Next**. The SSID group box appears.

Step 8 From the 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 From the Display Rule group box, you can do the following:

- Select the **Display Rule** radio button. You can select either **Everywhere** or **Near selected APs** radio button. By default, Display everywhere is selected.

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

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

- AP—Select those APs on which you want the advertisements to broadcast.
- Radio—Select the radio frequency on which you want the advertisements to be broadcasted. The service advertisement is displayed when the mobile device is near the radio band that you have selected. The possible values are 2.4 GHz or 5 GHz.
  - min RSSI—Enter a value for RSSI at which you want the service advertisemfm
  - ents to be displayed on the user interface.

Step 11 Click **Finish**.

Step 12 If you want to delete a policy, do the following in the Policy page:

a) Select the check box of the policy that you want to delete.
b) From the **Select a command** drop-down list, choose **Delete Provider**, and click **Go**.
c) Click **OK** to confirm the deletion.

Related Topics

Configure Mobile Concierge Using MSE, on page 61
Configure Venues for Mobile Concierge (MSE), on page 61
Configure Providers for Mobile Concierge (MSE), on page 63

Configure wIPS Using the MSE Wireless Security Configuration Wizard

The Wireless Security wizard page appears and allows you to perform the following wIPS related configurations:

- Allows rogue policy to detect and report ad hoc networks.
- Allows rogue rules to define rules to automatically classify rogue access points.
- Allows you to add new wIPS profiles.

Procedure

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

By default, the Before You Begin tab opens. The Before You Begin wizard page displays information about how to use the Wireless Security wizard and includes the following information:

- Rogue Policy—The Rogue Policy page enables you to configure the rogue policy. It has three pre-configured rogue policy settings for rogue detection and containment.
- Rogue Rules—The Rogue Rules page allows you to automatically classify rogue access points based on criteria such as authentication type, matching configured SSIDs, client count, and RSSI values. Rogue rules can be created to classify rogues as Malicious and Friendly.
- wIPS Profile—The wIPS Profile page provides several pre-defined profiles from which to choose. These profiles allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. The profile can be further customized by selecting the awIPS signatures to be detected and contained.
- Devices—The Devices page allows you to apply rogue policy, rogue rules, and wIPS profiles to controllers.

Step 2 Click **Next** to configure the Rogue Policy to detect and report ad hoc networks. This page enables you to configure the rogue policy (for access points and clients) applied to the controller.

- You can either set the policy settings to Low, High, or Critical by moving the Configure the rogue policy settings sliding bar with the mouse or select the Custom check box to configure the policy settings.s
- In the General group box, configure the following fields:
    - Rogue Location Discovery Protocol—Determines whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network. Choose one of the following from the drop-down list:
    - Disable—Disables RLDP on all access points.
    - All APs—Enables RLDP on all access points.
    - Monitor Mode APs—Enables RLDP only on access points in monitor mode.
- Expiration Timeout for Rogue AP and Rogue Client Entries—Set the expiration timeout (in seconds) for rogue access point entries. The valid range is 240 to 3600 seconds.
- Validate rogue clients against AAA—Select the Validate rogue clients against AAA check box to enable the AAA validation of rogue clients.
- Detect and report Adhoc networks—Select the Detect and report Adhoc networks check box to enable detection and reporting of rogue clients participating in ad hoc networking.

- Rogue Detection Report Interval—In the Rogue Detection Report Interval text box, enter the time interval in seconds at which the APs should send the rogue detection report to the controller. A valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.
- Rogue Detection Minimum RSSI—In the Rogue Detection Minimum RSSI text box, enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. A valid range is -70 dBM to -128 dBm. This feature is applicable to all the AP modes.
- Rogue Detection Transient Interval—In the Rogue Detection Transient Interval text box, enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only.
- In the Auto Contain group box, configure the following fields:
  - Rogue on Wire—Select the Rogue on Wire check box to auto contain those APs that are detected on the wired network.
  - Using our SSID—Select the Using our SSID check box.
  - Valid client on Rogue AP—Select the Valid client on Rogue AP check box to auto contain the valid clients from connecting to the rogue APs.
  - AdHoc Rogue—Select the AdHoc Rogue checkbox to auto contain adhoc rogue APs.
- Click Apply to apply the current rule to controllers. In the Devices wizard page, select the applicable controllers and click Apply to Controllers.

Step 3 Click **Next** to configure the rogue rules. This page enables you to define rules to automatically classify rogue access points. Prime Infrastructure applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

Step 4 Click **Create New** to create new rogue rules.The Add/Edit Rogue Rule window appears.

- In the General group box, configure the following fields:
  - **Rule Name**—Enter a name for the rule in the text box.
  - **Rule Type**—Choose Malicious or Friendly from the drop-down list.

Note Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category. Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.

- Match Type—Choose Match All Conditions or Match Any Condition from the drop-down list.
- In the Rogue Classification Rule group box, configure the following fields:
  - Open Authentication—Select the Open Authentication check box to enable Open Authentication.
  - Match Managed AP SSID—Select the Match Managed AP SSID check box to enable the matching of managed AP SSID rule condition.

    Note Managed SSID are the SSIDs configured for the WLAN and is known to the system.

  - Match User Configured SSID (Enter one per line)—Select the Match User Configured SSID check box to enable the matching of user configured SSID rule condition.

    Note User Configured SSID are the SSIDs that are manually added. Enter the User Configured SSIDs (one per line) in the Match User Configured SSID text box.

- Minimum RSSI—Select the Minimum RSSI check box to enable the Minimum RSSI threshold limit.

  Note Enter the minimum RSSI threshold level (dB) in the text box. The detected access point is classified as malicious if it is detected above the indicated RSSI threshold.

- Time Duration—Select the Time Duration check box to enable the Time Duration limit.

  Note Enter the time duration limit (in seconds) in the text box. The detected access point is classified as malicious if it is viewed for a longer period of time than the indicated time limit.

- Minimum Number Rogue Clients—Select the Minimum Number Rogue Clients check box to enable the Minimum Number Rogue Clients limit.

  Note Enter the minimum number of rogue clients allowed. The detected access point is classified as malicious if the number of clients associated to the detected access point is greater than or equal to the indicated value.

- Click **Ok** to save the rule or Cancel to cancel the creation or changes made to the current rule. You are returned to the Rogue Rules page and the newly added rogue rule is listed.
- Click **Apply** to apply the current rule to controllers. In the Devices wizard page, select the applicable controllers and click Apply to Controllers.

Step 5 Click **Next** to configure the wIPS profiles. Prime Infrastructure provides several pre-defined profiles from which to choose. These profiles (based on customer types, building types, industry types, and so on) allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. You can use a profile 'as is' or customize it to better meet your needs.

Step 6 For more information on configuring the wIPS profile, see the Configuring wIPS and Profiles section.

Step 7 After configuring wIPS profile, click **Next** to open the Devices page where you can select the controllers to apply the settings.

Configure Connected Mobile Experiences

Cisco Connected Mobile Experiences (CMX) is a smart Wi-Fi solution that uses the wireless infrastructure to detect and locate users mobile devices. With it, you can directly deliver content to smartphones and tablets that is personalized to user preferences. Cisco CMX is a software solution that integrates with other components, such as the Cisco Mobility Services Engine (MSE) for location identification and the Cisco Enterprise Mobility Services Platform (EMSP) for mobile app development, distribution, and management.

Important

- Prime Infrastructure 3.2 supports integration with CMX 10.3. It uses the below queries to query CMX:
  - /api/config/v1/version/image (to get CMX version)
  - /api/config/v1/campuses/import (to import map file into CMX)
- Prime Infrstructure 3.5 does not support CMX versions 10.3 and 10.4. So, when upgrading Prime Infrastructure to version 3.5, you also need to upgrade CMX to 10.5.
- The file storage limit for Import Map to CMX is ten map export files. If you try to import additional files, a message asking you to remove one of the existing files will be displayed.
- CMX should be configured in location mode and loaded with maps from Prime Infrastructure before viewing the CMX clients in Prime Infrastructure
- Prime Infrastructure 3.4 onwards, Site Map synchronized with CMX 10.4 and above displays positions of RFID Tags, Rogue Clients, Rogue APs, and Clients (associated and not associated).
- If Prime Infrastructure has both MSE and CMX added, the floor map can be synchronized only to either of them. So the corresponding clients in this floor can be tracked only by any one of them.
- Changes done to maps in Prime Infrastructure are not synchronised with CMX, as there is no periodic task to update the information. Maps have to be re-imported to CMX to retrieve the updated information.
- Prime Infrastructure does an API query on CMX when the map page is open and it refreshes based on the configured map refresh interval.

Related Topics

Manage CMX in Prime Infrastructure , on page 68

Manage CMX in Prime Infrastructure

To add, edit, and delete a CMX device and to import site maps from Prime Infrastructureto CMX:

Procedure

Step 1 To add a device, choose **Services** > **Mobility Services** > **Connected Mobile Experiences**.

Alternately, you can click the Manage CMX link in the **Services** > **Mobility Services** > **Mobility Service Engine** page.

Step 2 Click **Add**.

Step 3 Enter the following details:

- IP address
- Device Name
- CMX Username (GUI Credentials)
- CMX password (GUI Credentials)

- SSH User (optional)
- SSH Password (optional)
- Name of the Owner (optional)

Step 4 Click **Save** to add the device.

Step 5 To edit the device parameters, choose **Services** > **Mobility Services** > **Connected Mobile Experiences**.

Step 6 Click **Edit**.

Step 7 Edit any or all of the following parameters:

- CMX Username (GUI Credentials)
- CMX password (GUI Credentials)
- SSH User (optional)
- SSH Password (optional)
- Name of the Owner (not mandatory)

Step 8 Click **Update** to save the new parameters or **Cancel** to go back to the previous parameters.

Step 9 To delete any device, choose **Services** > **Mobility Services** > **Connected Mobile Experiences**.

Step 10 Click **Delete**.

Step 11 Select the devices you want to delete and click **Delete** > **Ok**.

Step 12 To import the site maps into CMX, choose **Services** > **Mobility Services** > **Connected Mobile Experiences**. select a CMX and click **Import Map to CMX**

Note If the CMX is in Presence mode, map will not be visible in CMX, but will be visible in Location mode.

Step 13 Choose a map and click **Import Map to CMX**

Note You can also add map files to Prime Infrastructurewith the **Export Map from PI** button in the List CMX page.

Step 14 To create a new map file, click **Export From PI** in the **Import Map to CMX** window.

Step 15 In the Maps page, select the map and save it to Prime Infrastructure.

On syncing, CMX can track the following parameters:

- Clients
- Interferers
- Rogue APs
- Rogue Clients
- RFID Tags