Prime Infrastructure Services

This chapter describes the role of the Cisco mobility services engine (MSE), within the overall Cisco Unified Wireless Network (CUWN).

- Mobility Services, page 16-719
- Mobile Concierge Service, page 16-818
- Identity Services, page 16-826

Mobility Services

This section briefly describes the CAS, wIPS, Mobile Concierge service, and Location Analytics service that Cisco Prime Infrastructure supports and provides the mobility procedures that are common across all services.

CAS

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

Note

You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points. Licenses for tags and clients are offered independently. See the Cisco 3355 Mobility Services Engine Release Note at the following URL for details on tag and client licenses:


wIPS

Cisco Adaptive Wireless IPS (wIPS) is an advanced approach to wireless threat detection and performance management. wIPS combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention.
Note

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

Mobile Concierge Service

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

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

Location Analytics Service

The Location Analytics service analyzes wireless device location information in a particular network. The Location Analytics service uses the data provided by the Cisco Mobility Services Engine (MSE) to calculate the location of Wi-Fi devices in the WLAN.

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 Location Analytics service helps the airport authorities or the building owners to understand passengers or customers within their building. This helps them improve the signage, make changes to the underutilized areas, and so on.

Cisco Context-Aware Mobility Solution

The foundation of the CAM solution is the controller-based architecture of the CUWN. The CUWN contains the following primary components:

- Cisco Prime Infrastructure, page 721
- WLAN Controllers, page 721
- Access Points, page 721
- Cisco 3300 Series Mobility Services Engines, page 722
Cisco Prime Infrastructure

With the Prime Infrastructure, network administrators have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and wired and wireless LAN systems management. Robust graphical interfaces make wired and wireless LAN deployment and operations simple and cost-effective. Detailed trending and analysis reports make the Prime Infrastructure vital to ongoing network operations.

WLAN Controllers

The WLAN controllers are highly scalable and flexible platforms that enables system wide services for mission-critical wireless in medium to large-sized enterprises and campus environments. Designed for 802.11n performance and maximum scalability, the WLAN controllers offer enhanced uptime with the ability to simultaneously manage from 5000 access points to 250 access points; superior performance for reliable streaming video and toll quality voice; and improved fault recovery for a consistent mobility experience in the most demanding environments.

The Prime Infrastructure supports the Cisco wireless controllers that help reduce the overall operational expense of Cisco Unified Networks by simplifying network deployment, operations, and management. The following WLAN controllers are supported in the Prime Infrastructure:

- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 2500 Series Wireless Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless Controllers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless Services Module 2 (WiSM2) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless Controller on SRE for ISR G2 Routers
- Cisco Flex 7500 Series Wireless Controllers
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers

Access Points

The following access points are supported:

- Cisco Aironet 801, 802, 1000, 1040, 1100, 1130, 1140, 1200, 1230, 1240, 1250, 1260, 1310, 1500, 1524, 1552, 1600i, 1600e, 2600i, 2600e, 3500i, 3500e, 3500p, 3600i, and 3600e Series Lightweight Access Points.
- Cisco Aironet 1040, 1100, 1130, 1141, 1142, 1200, 1240, 1250, and 1260.
- Cisco 600 Series OfficeExtend Access Points.
Cisco 3300 Series Mobility Services Engines

The Cisco Mobility Services Engine operates with CAS, which is a component of the CAM solution. There are two models of the mobility services engine:

- Cisco 3355 Mobility Services Engine
- Cisco Virtual Appliance

Accessing Services

You can access the MSE installation guides as follows:

MSE 3355 Installation guide:

MSE Services Coexistence

With the MSE 6.0 and later, you can enable multiple services (Context-Aware Service and wIPS) to run concurrently. Before Version 6.0, mobility services engines only supported one active service at a time.

The following must be considered with coexistence of multiple services:

- Coexistence of services might be impacted by license enforcement. As long as the license is not expired, you can enable multiple services.

Note
The CAS license is now called Base location license.

- Expired evaluation licenses prevent the service from coming up.
- If a Base location license is added or removed, this process restarts all services on the mobility services engine including wIPS. If a wIPS license is added or removed, the process does not impact CAS; only wIPS restarts.
- Other services can be enabled in evaluation mode even if a permanent license for the maximum number of elements has been applied.

Whenever one of the services has been enabled to run with its maximum license, another service cannot be enabled to run concurrently because the capacity of the MSE is not sufficient to support both services concurrently.

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

Viewing Current Mobility Services

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

The Mobility Services Engines page provides the following information and features for each device:
Chapter 16 Prime Infrastructure Services

Mobility Services

- Device Name—User-assigned name for the mobility services engine. Click the device name to see and manage mobility services engine details. See the “Managing System Properties for a Mobility Services Engine” section on page 16-745 for more information.
- Device Type—Indicates the type of mobility services engine. Indicates whether the device is a virtual appliance or not.
- IP Address—Indicates the IP address for the mobility services engine.
- Version—Indicates the version number of the mobility services engine.
- Reachability Status—Indicates whether or not the mobility services engine is reachable.
- Secondary Server—Indicates whether or not the secondary server is installed.
- Mobility Service:
  - Name—Indicates the name of the mobility service.
  - Admin Status—Indicates whether the mobility service is enabled or disabled.
  - Service Status—Indicates whether the mobility service is currently up or down.
- Select a command drop-down list:
  - Add Location Server
  - Add Mobility Services Engine—Contains Context-Aware Service, Cisco Adaptive Wireless IPS (wIPS) service, Mobile Concierge Service, and Location Analytics Service.
  - Delete Service(s)
  - Synchronize Services
  - Synchronization History
  - Edit Configuration

Note Location and mobility services engine features of the Prime Infrastructure do not support partitioning.

Adding a Mobility Services Engine

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.

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

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

Note The Services > Mobility Services Engine page is available only in root virtual domain.
To add a mobility services engine to the Prime Infrastructure, log into the Prime Infrastructure and follow these steps:

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

**Step 2** Choose Services > Mobility Services Engines to display the Mobility Services page.

**Step 3** From the Select a command drop-down list, choose Add Mobility Services Engine, and click Go. The Add Mobility Services Engine page appears.

**Step 4** Enter the following information:

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

**Note** A mobility services engine is added only if a valid IP address is entered. The Device Name helps you distinguish between devices if you have multiple Prime Infrastructures with multiple mobility services engines, but it is not considered when validating a mobility services engine.

- **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.

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

- **HTTPS**—This is used for communication between the Prime Infrastructure and mobility services engine. By default, the Prime Infrastructure uses HTTPS to communicate with MSE.

- Select the Delete synchronized service assignments check box if you want to permanently remove all service assignments from the mobility services engine.

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

**Step 5** Click Next. The Prime Infrastructure automatically synchronizes the selected elements with the MSE.

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

### Configuring Services for MSE

**Step 6** To enable a service on the mobility services engine, select the check box next to the service. Services include Context-Aware Service, wIPS, Mobile Concierge Service, Location Analytics Service, and Billboard Service.

You can choose CAS to track clients, rogues, interferers, wired clients, and tags. When you select Context Aware Service check box, the following is displayed.
- Cisco Context-Aware Engine for Clients and Tags—The Cisco Context-Aware engine is used to track clients.

or

- Partner Tag Engine—The Partner Engine is used to tags.

**Configuring MSE Tracking and History Parameters**

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

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

**Step 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**

**Note** 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. For more information, please visit http://www.meridianapps.com/mse

Step 15 Once you assign maps to the MSE, the Mobile App Enablement page appears.

Step 16 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 17 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 18 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 19 Enter the street address of your location in the Street Address text box.

Step 20 Enter the phone number where Meridian can reach you for additional information in the Phone Number text box.

Step 21 Click Advanced to open the Advanced pane.

Step 22 If you want MSE to send real-time notifications to Meridian whenever 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 the Prime Infrastructure and synced to the MSE.

Step 23 Click OK after selecting zones and floors.

Step 24 Click Save.

Step 25 Click Done to save the MSE settings.

Deleting an MSE License File

To delete an MSE license file, follow these steps:

Note The Services > Mobility Services Engine page is available only in root virtual domain in Release 7.3.
Step 1  Choose Services > Mobility Service Engine.
The Mobility Services page appears.

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

Step 3  From the Select a command drop-down list, choose Edit Configuration.
The Edit Mobility Services Engine dialog box appears.

Step 4  Click Next in the Edit Mobility Services Engine dialog box.
The MSE License Summary page appears.

Step 5  Choose the MSE license file that you want to delete in the MSE License Summary page.

Step 6  Click Remove License.

Step 7  Click OK to confirm the deletion or Cancel to close this page without deleting the license.

Step 8  Click Next to enable services on the mobility services engine.

Deleting a Mobility Services Engine from the Prime Infrastructure

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

Step 1  Choose Services > Mobility Services Engine.
The Mobility Services page appears.

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

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

Step 4  Click Go.

Step 5  Click OK to confirm that you want to delete the selected mobility services engine from the Prime Infrastructure database.

Step 6  Click Cancel to stop the deletion.

Registering Product Authorization Keys

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

CAS element and wIPS PAKs are registered with Cisco.

Tag PAKs are registered with AeroScout.

Note  If you do not have a PAK, you can use the sales order number to retrieve the PAK. See the “Retrieving a PAK” section on page 16-728 for more information.
To register for a Product Authorization Key (PAK) and to obtain a license file for install, follow these steps:

**Step 1**

**Step 2**
Enter the PAK, and click **Submit**.

**Step 3**
Verify the license purchase. Click **Continue** if correct. The licensee entry page appears.

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

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

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

**Step 5**
Select the **Agreement** check box. Registrant information appears beneath the Agreement check box. Modify the information as necessary.

**Note** Ensure that the phone number does not include any characters in the string for the registrant and end user. For example, enter 408 555 1212 rather than 408.555.1212 or 408-555-1212.

**Step 6**
If the registrant and end user are not the same person, select the **Licensee (End-User)** check box beneath registrant information and enter the end user information.

**Step 7**
Click **Continue**. A summary of entered data appears.

**Step 8**
In the Finish and Submit page, review registrant and end-user data. Click **Edit Details** to correct any information, if necessary.

**Step 9**
Click **Submit**. A confirmation page appears.

---

**Retrieving a PAK**

If you do not have a PAK, you can use the sales order number to retrieve the PAK:

**Step 1**
Go to the Sales Order Status Tool at the following URL: [http://tools.cisco.com/qtc/status/tool/action/LoadOrderQueryScreen](http://tools.cisco.com/qtc/status/tool/action/LoadOrderQueryScreen).

**Step 2**
After logging in, choose **Sales Order (SO)** from the Type of Query drop-down list.

**Step 3**
Enter the sales order number in the Value text box.

**Note** The **Date Submitted** fields are not required for this inquiry.

**Step 4**
Select the **Show Serial Number** check box.

**Step 5**
Select the **Orders** radio button, if not already selected.

**Step 6**
Choose **Screen** from the Deliver through drop-down list.
Step 7 Click Search. Detailed information on the mobility services engine order appears.
Step 8 Click Line 1.1 in the table.
Step 9 In Product column (second line), copy the PAK number (starts with 3201J) that you want to register to obtain the license.

Installing Device and wIPS License Files

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

Note Tag licenses are installed using the AeroScout System Manager. To register your tag PAK, go to this URL:
http://www.aeroscout.com/content/support

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

Note The Administration > Licensing page is available only in root virtual domain in Release 7.3.

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

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

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

Adding a Location Server

To add a location server, follow these steps:

Step 1 Choose Services > Mobility Services.
Step 2 From the Select a command drop-down list, choose Add Location Server.
Step 3 Click Go.
Step 4 Enter the following information:
- Device Name
- IP Address
- Contact Name
- User Name
- Password
- Port
- HTTPS—When enabled, HTTPS is used for communication between the Prime Infrastructure and location server.

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

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

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

**Note**
After adding a location server, it must be synchronized with the Prime Infrastructure. See the “Synchronizing Services” section on page 16-730 for more information.

**Note**
Location and mobility services engine features of the Prime Infrastructure do not support partitioning.

### Synchronizing Services

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

**Note**
The Synchronize Services page on the Services tab is available only in the root virtual domain in Release 7.3.

### Keeping Mobility Services Engines Synchronized

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

After adding a mobility service engine to the Prime Infrastructure, you can synchronize network designs (campus, building, floor, and outdoor maps), event groups, controller information (name and IP address), or wired switches to the mobility services engine.

**Note**
Be sure to verify software compatibility between the controller, the Prime Infrastructure, and the mobility services engine before performing synchronization. See the latest mobility services engine release notes at the following URL: [http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html](http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html).
Chapter 16      Prime Infrastructure Services

Note

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

Synchronizing the Prime Infrastructure and a Mobility Services Engine

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

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

- 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 a mobility services engine. 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 mobility services engine can be synchronized with Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports.
  - The mobility services engine can also be synchronized with the following Catalyst 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.

Note

Be sure to verify software compatibility between the controller, the Prime Infrastructure, and the mobility services engine before synchronizing. See the latest mobility services engine release notes at the following URL:

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

Synchronizing Prime Infrastructure Network Designs, Controllers, Wired Switches, or Event Groups

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

**Step 1** Choose **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 a mobility services engine, from the left sidebar menu, choose **Network Designs**.

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

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

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

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

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

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

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

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

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:

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

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

**Step 3** Click Change MSE Assignment.

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

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

- **Save**—Saves the mobility services engine assignment. The following message appears in the Messages column of the Controllers page:
  
  To be assigned - Please synchronize.

- **Cancel**—Discards the changes to the mobility services engine 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 mobility services engine is communicating with each of the controllers for only the chosen service. This can be done by clicking the NMSP status link in the status page.

**Note** After Synchronizing a controller, verify that the timezone is set on the associated controller. See the “Setting and Verifying the Timezone on a Controller” section on page 16-734 for more information.

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

To unassign a network design, controller, wired switch, or event group from a mobility services engine, follow these steps:
Step 1  On the respective tabs, click one or more elements, and click **Change MSE Assignment**. The Choose Mobility Services Engine dialog box appears.

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

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

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

---

**Working with Third-Party Elements**

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

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

---

Step 1  Choose **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.

---

**Setting and Verifying the Timezone on a Controller**

For controller Releases 4.2 and later, if a mobility services engine (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:

---

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

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

Mobility Services

Note  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:

(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:

Note  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.

(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:

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

Note  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.

Configuring Smart Mobility Services Engine Database Synchronization

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

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

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

To configure smart synchronization, follow these steps:
Choose Administration > Background Tasks.

The Background Tasks summary page appears.

Select the Mobility Service Synchronization check box.

The Mobility Services Synchronization page appears.

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

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 a mobility services engine. However, out-of-sync alarms are still generated for these unassigned elements. For smart synchronization to apply to these elements, you need to manually assign them to a mobility services engine.

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

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

By default, smart-sync is disabled.

Click Submit.

See the “Smart Controller Assignment and Selection Scenarios” section on page 16-736 for more information on smart controller assignment and selection scenarios.

**Smart Controller Assignment and Selection Scenarios**

**Scenario 1**

If a floor having at least one access point from a controller is chosen to be synchronized with the mobility services engine 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 mobility services engine for CAS service.

**Scenario 2**

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

**Scenario 3**

An access point is added to a floor and is assigned to an mobility services engine. If that access point is moved from controller A to controller B, then controller B is automatically synchronized to the mobility services engine.
If all access points placed on a floor which is synchronized to the mobility services engine are deleted then that controller is automatically removed from mobility services engine assignment or unsynchronized.

**Out-of-Sync Alarms**

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

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

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

- The mobility services engine is deleted

**Note** When you delete a mobility services engine, the out-of-sync alarms for that system is also deleted. In addition, if you delete the last available mobility services engine, 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)

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

**Viewing Mobility Services Engine Synchronization Status**

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

To view synchronization status, follow these steps:

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

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

For each of the elements, the Sync. Status column shows the synchronization status. A green two-arrow icon indicates that its corresponding element is synchronized with the specified server such as a mobility services engine. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a provided server.
Note: 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 mobility services engine the floor is currently assigned to. You can also change mobility services engine assignment from this page.

Viewing Synchronization History

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

Note: 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.

Viewing Notification Statistics

You can view the notification statistics for a specific mobility services engine. To view the Notification Statistics for a specific mobility services engine:

Choose Services > Mobility Services > MSE-name > Context Aware Service > Notification Statistics where MSE-name is the name of a mobility services engine.

Table 16-1 describes the fields in the Notification statistics page.

<table>
<thead>
<tr>
<th>Table 16-1 Notification Statistics fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>Summary</td>
</tr>
<tr>
<td>Destinations</td>
</tr>
<tr>
<td>Total</td>
</tr>
<tr>
<td>Unreachable</td>
</tr>
<tr>
<td>Notification Statistics Summary</td>
</tr>
<tr>
<td>Destination Address</td>
</tr>
<tr>
<td>Destination Port</td>
</tr>
</tbody>
</table>
Chapter 16  Prime Infrastructure Services

Mobility Services

Table 16-1  Notification Statistics fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td></td>
</tr>
<tr>
<td>Destination Type</td>
<td>The type of the destination. Example: SOAP_XML</td>
</tr>
<tr>
<td>Destination Status</td>
<td>Status of the track definition. Track notification status can be either Enabled or Disabled.</td>
</tr>
<tr>
<td>Last Sent</td>
<td>The date and time at which the last notification was sent to the destination device.</td>
</tr>
<tr>
<td>Last Failed</td>
<td>The date and time at which the notification failed.</td>
</tr>
<tr>
<td>Track Definition (Status)</td>
<td></td>
</tr>
<tr>
<td>Total Count</td>
<td>The total count of notifications sent to the destination. Click the count link to view the notification statistics details of the destination device.</td>
</tr>
</tbody>
</table>

Configuring High Availability

The mobility services engine is a platform for hosting multiple mobility applications. Every active MSE is backed up by another inactive instance. The active MSE is called the primary MSE and the inactive MSE is called the secondary MSE.

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

This section provides an overview of the high availability architecture:

- Every active primary MSE is backed up by another inactive instance. The purpose of the secondary MSE is to monitor the availability and state of the primary MSE. The secondary MSE becomes active only after the failover procedure is initiated.
- The failover procedure can be manual or automatic.
- One secondary MSE can support two primary MSES.
- There is one software and database instance for each registered primary MSE.

Note

The high availability on the Services tab is available only in the root virtual domain in Release 7.3.

Pairing Matrix

Table 16-2 provides pairing matrix information.
Both the health monitor IP and Virtual IP should be accessible from the Cisco Prime Infrastructure.

The health monitor IP and virtual IP should always be different. The health monitor and virtual interface can be on the same interface or different interfaces.

You can use either manual or automatic failover. Failover should be considered temporary. The failed MSE should be restored to normal as soon as possible, and failback will reinitiate. The longer it takes to restore the failed MSE, the longer the other MSEs sharing the secondary MSE must run without failover support.

You can use either manual or automatic failback.

Both the primary and secondary MSE should be running the same software version.

High availability over WAN is not supported.

High Availability over LAN is supported only when both the primary and secondary MSE are in the same subnet.

The ports over which the primary and secondary MSEs communicate must be open (not blocked with network firewalls, application firewalls, gateways, and so on).

Failover Scenario for High Availability

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

One secondary MSE can back up multiple primary MSEs.

The primary MSE is confirmed as non-functioning (hardware fail, network fail, and so on) by the health monitor on the secondary MSE.

If automatic failover has been enabled, the secondary MSE is started immediately and uses the corresponding database of the primary MSE. If automatic failover is disabled, an e-mail is sent to the administrator asking if they want to manually start failover.

When the manual failover is configured, an e-mail is sent only if the e-mail is configured for MSE alarms. When manual failover is configured and not invoked, there is no need for failback.

Failback is invoked and the primary MSE assumes all the operations.

The result of the failover operation is indicated as an event in the Health Monitor UI, and critical alarm is sent to the administrator.

Table 16-2  Pairing Matrix

<table>
<thead>
<tr>
<th>Primary Server Type</th>
<th>Secondary Server Type</th>
<th>VA-2</th>
<th>VA-3</th>
<th>VA-4</th>
<th>VA-5</th>
</tr>
</thead>
<tbody>
<tr>
<td>3355</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>VA-2</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>VA-3</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>VA-4</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>VA-5</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>

Guidelines and Limitations for High Availability

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

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

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

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

HA Licensing

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

Configuring High Availability on the MSE

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

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

Note

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

Note

By default, all MSEs are configured as primary.

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

Step 1
Ensure that the network connectivity between the primary and secondary is functioning and that all the necessary ports are open.

Step 2
Install the correct version of MSE on the primary MSE.

Step 3
Make sure that the same MSE release version that is loaded on the other primary MSE and secondary MSE is also loaded on the new primary MSE.

Step 4
On the intended primary MSE, enter the following command:

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

Welcome to the appliance setup.
Please enter the requested information. At any prompt, enter ^ to go back to the previous prompt. You may exit at any time by typing <Ctrl+C>.
You will be prompted to choose whether you wish to configure a
Step 5  Configure the hostname:

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

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

Step 6  Configure the domain name:

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

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

Step 7  Configure the HA role:

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

Health monitor interface holds physical IP address of this MSE server. This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to communicate among themselves.

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

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

Step 8  Configure Ethernet interface parameters:

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

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

Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
Follow Step 10 through Step 13 to configure the secondary MSE.

Step 10
Configure the hostname for the secondary MSE:

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

Step 11
Configure the domain name:

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

Step 12
Configure the HA role:

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

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

Step 13
Configure Ethernet interface parameters:

Select direct connect interface [eth0/eth1/none] [none]: eth1
Enter a Virtual IP address for first this primary MSE server
Enter Virtual IP address [172.19.35.61]:
Enter the network mask for IP address 172.19.35.61:
Enter network mask [255.255.254.0]:
Current IP address=[172.19.35.127]
Current gateway address=[172.19.34.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:

Step 14
Once you have configured both the primary MSE and secondary MSE, the Prime Infrastructure UI should be used to set up a pairing between the primary and secondary MSE.

Step 15
Once the primary MSE is added successfully, choose Services > High Availability or click the primary MSE device in the Services > Mobility Services Engine page, and choose HA Configuration > Service High Availability from the left sidebar menu.
The HA Configuration page appears.

Step 16
Enter the secondary device name with which you want to pair the primary MSE.

Step 17
Enter the secondary IP address which is the health monitor IP address of the secondary MSE.

Step 18
Enter the secondary password. This is the Prime Infrastructure communication password configured on the MSE.
Step 19 Specify the failover type. You can choose either Manual or Automatic from the Failover Type drop-down list. After 10 seconds, the system fails over. The secondary server waits for a maximum of 10 seconds for the next heartbeat from the primary server. If it does not get the heartbeat in 10 seconds, it declares a failure.

Step 20 Specify the failback type by choosing either Manual or Automatic from the Failback Type drop-down list.

Step 21 Specify the Long Failover Wait in seconds.

Step 22 Click Save.

Step 23 To check whether the heartbeat is received from the primary MSE or not, choose Services > Mobility Services Engine, and click Device Name to view the configured parameters.

Step 24 Choose HA Configuration > Service High Availability from the left sidebar menu.

---

Viewing Configured Parameters for High Availability

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

Step 1 Choose Services > High Availability.

Step 2 Click Device Name to view its configured parameters.

Step 3 Choose Services High Availability > HA Configuration from the left sidebar menu. The HA Configuration page shows the following information:

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

---

Viewing High Availability Status

To view the high availability status, follow these steps:

Step 1 Choose Services > High Availability.

Step 2 Click Device Name to view the desired status.

The HA Configuration page appears.
Step 3  Choose **Services High Availability > HA Status** from the left sidebar menu. The HA Configuration page shows the following information:

- Current high Availability Status
  - Status—Shows whether the primary and secondary MSE instances are correctly synchronized or not.
  - Heartbeats—Shows whether the heartbeat is received from the primary MSE or not.
  - Data Replication—shows whether the data replication between the primary and secondary databases is happening or not.
  - Mean Heartbeat Response Time—shows the mean heartbeat response time between the primary and secondary MSE instance.
- Event Log—Shows all the events generated by the MSE. It shows the last 20 events.

---

**Managing System Properties for a Mobility Services Engine**

You can manage the system properties of a mobility services engine using the Prime Infrastructure. This section describes the various system properties of a mobility services engine.

**Editing General Properties for a Mobility Services Engine**

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

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

---

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

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

On the General tab, the following read-only server details appear:

- Device Name
- Device Type
- Device UDI

**Note**  For licensing, the Device UID is the string between double quote characters (including spaces in the end, if any). Exclude the double quote characters using copy-paste.

- Version
- Start Time
- IP Address

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.

  **Note** 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 mobility services engine. This option shows up only if the delete synchronized service assignments check box was unselected while adding a mobility services engine.

  **Note** The Prime Infrastructure always uses HTTPS to communicate with a mobility services engine.

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

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

**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, mobility services engines 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

**Note** Use the Click here link to view mobility services engine licensing details.

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

**Note** Use the Click here link to view mobility services engine licensing details.

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

---

**Editing NMSP Parameters for a Mobility Services Engine**

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 the 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 in the Prime 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:

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

**Step 2**
Click the name of the mobility services engine 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 No change in the default parameter values is recommended 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.

  **Note** If a network is experiencing slow response, you can increase the values of the echo interval, neighbor dead interval and the response timeout values to limit the number of failed echo acknowledgements.

- **Neighbor Dead Interval**—The number of seconds that the mobility 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.

  **Note** 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 the Prime Infrastructure and mobility service databases.

---

**Viewing Active Session Details for a Mobility Services Engine**

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

To view active user sessions, follow these steps:

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

**Step 2** Click the name of the mobility service.

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

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

Viewing and Adding Trap Destinations for a Mobility Services Engine

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

To view or manage trap destination for a mobility services engine, follow these steps:

Step 1 Choose Services > Mobility Services Engines.
Step 2 Click the name of the mobility service.
Step 3 From the left sidebar menu, choose System > Trap Destinations.

The 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.

To add a trap destination, follow these steps:

Step 1 Choose Services > Mobility Services.
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 Table 16-3).

<table>
<thead>
<tr>
<th>Table 16-3</th>
<th>Add Trap Destination Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address for the trap destination</td>
</tr>
<tr>
<td>Port No.</td>
<td>Port number for the trap destination. The default port number is 162.</td>
</tr>
<tr>
<td>Destination Type</td>
<td>This field is not editable and has a value of Other.</td>
</tr>
</tbody>
</table>
Click **Save** to save the changes or **Cancel** to discard the changes.

### Table 16-3  Add Trap Destination Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snmp Version</td>
<td>Select either v2c or v3.</td>
</tr>
</tbody>
</table>

The following set of fields appear only if you select v3 as the SNMP version.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Username for the SNMP Version 3.</td>
</tr>
<tr>
<td>Security Name</td>
<td>Security name for the SNMP Version 3.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>HMAC-MD5</td>
</tr>
<tr>
<td></td>
<td>HMAC-SHA</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>Authentication password for the SNMP Version 3.</td>
</tr>
<tr>
<td>Privacy Type</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>CBC-DES</td>
</tr>
<tr>
<td></td>
<td>CFB-AES-128</td>
</tr>
<tr>
<td></td>
<td>CFB-AES-192</td>
</tr>
<tr>
<td></td>
<td>CFB-AES-256</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>Privacy password for the SNMP Version 3.</td>
</tr>
</tbody>
</table>

**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 mobility services engine.
  - Version Identifier (VID)—The version number of the mobility services engine.
  - Serial Number (SN)—Serial number of the mobility services engine.

- Advanced Commands
  - Reboot Hardware—Click to reboot the mobility service hardware. See the “Rebooting the Mobility Services Engine Hardware” section on page 16-751 for more information.
  - Shutdown Hardware—Click to turn off the mobility service hardware. See the “Shutting Down the Mobility Services Engine Hardware” section on page 16-751 for more information.
  - Clear Database—Click to clear the mobility services database. See the “Clearing the Mobility Services Engine Database” section on page 16-752 for more information. Unselect the Retain current service assignments in the Prime Infrastructure check box to remove all existing service assignments from the 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 the Prime Infrastructure and mobility service databases.

Rebooting the Mobility Services Engine Hardware

If you need to restart a mobility services engine, follow these steps:

1. Choose Services > Mobility Services Engines.
2. Click the name of the mobility services engine that you want to reboot.
3. Click System.
4. Click Advanced Parameters.
5. In the Advanced Commands dialog box, click Reboot Hardware.
6. Click OK to confirm that you want to reboot the mobility services engine hardware.

The rebooting process takes a few minutes to complete.

Shutting Down the Mobility Services Engine Hardware

If you need to shut down a mobility services engine, follow these steps:

1. Choose Services > Mobility Services Engines.
2. Click the name of the mobility services engine that you want to shut down.
3. Click System.
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 mobility services engine.

---

**Clearing the Mobility Services Engine Database**

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

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

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

**Step 3** 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** check box to remove all existing service assignments from the Prime Infrastructure and MSE.

The resources have to be reassigned in the **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 mobility services engine database.

---

**Working with Logs**

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

**Configuring Logging Options**

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

To configure logging options, follow these steps:

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

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

**Step 3** Choose **System > Logs**. The advanced parameters for the selected mobility services engine appear.

**Step 4** Choose the appropriate options from the Logging Level drop-down list.

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

All log records with a log level of Error or 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 the “**Downloading Mobility Services Engine Log Files**” section on page 16-753 for more information.

Step 8  In the Log File group box, enter the following:

- The number of log files to be maintained in the mobility services engine. You can maintain a minimum of 5 log files and a maximum of 20 log files in the mobility services engine.
- The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.

Step 9  In the MAC Address Based Logging 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 the “**MAC Address-based Logging**” section on page 16-753 for more information on MAC Address-based logging.

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

**MAC Address-based Logging**

This feature allows you to create log files that are specific to an entity whose MAC address is specified. The log files are created in the loserver directory under the following path:

```
/opt/mse/logs/loserver
```

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.

**Downloading Mobility Services Engine Log Files**

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

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

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

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

Step 3  From the left sidebar menu, choose **Logs**.

Step 4  Click **Download Logs**.
Managing User and Group Accounts for a Mobility Services Engine

This section describes how to configure and manage users and groups on the mobility services engine.

This section describes how to add, delete, and edit users for a mobility services engine.

Note
See the “Viewing Active Session Details for a Mobility Services Engine” section on page 16-748 for information on viewing active sessions for each user.

• Managing Group Accounts—This section describes how to add, delete, and edit user groups for a mobility services engine and contains the following topics:
  - Adding User Groups, page 16-755
  - Deleting User Groups, page 16-756
  - Editing Group User Permissions, page 16-756

Adding Users for a Mobility Services Engine

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

Step 1  Choose Services > Mobility Services Engines.
Step 2  Click the device name of the mobility services engine that you want to edit.
Step 3  From the left sidebar menu, choose Systems > Accounts > Users.
Step 4  From the Select a command drop-down list, choose Add User.
Step 5  Click Go.
Step 6  Enter the username in the Username text box.
Step 7  Enter a password in the Password text box.
Step 8  Enter the name of the group to which the user belongs in the Group Name text box.
Step 9  Choose a permission level from the Permission drop-down list.

There are three permission levels to choose from: Read Access, Write Access, and Full Access (required for Prime Infrastructure to access a mobility services engine).

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 mobility services engine settings.

Step 10  Click Save to add the new user to the mobility services engine.
Deleting Users

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

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

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

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

**Step 4** Select the check box(es) of the user(s) that you want to delete.

**Step 5** From the Select a command drop-down list, choose **Delete User**.

**Step 6** Click **Go**.

**Step 7** Click **OK** to confirm that you want to delete the selected users.

Editing User Properties

To change user properties, follow these steps:

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

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

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

**Step 4** Click the username of the user that you want to edit.

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

**Step 6** Click **Save** to apply your change.

Adding User Groups

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

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

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

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

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

**Step 5** Click **Go**.

**Step 6** Enter the name of the group in the **Group Name** text box.

**Step 7** Choose a permission level from the **Permission** drop-down list.

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

**Step 8** Click **Save** to add the new group to the mobility services engine.
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 mobility services engine settings.

Deleting User Groups

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

Step 1  Choose Services > Mobility Services.
Step 2  Click the device name of the mobility services engine that you want to edit.
Step 3  From the left sidebar menu, choose Systems > Accounts > Groups.
Step 4  Select the check box(es) of the group(s) that you want to delete.
Step 5  From the Select a command drop-down list, choose Delete Group.
Step 6  Click Go.
Step 7  Click OK to confirm that you want to delete the selected users.

Editing Group User Permissions

To change user group permissions, follow these steps:

Step 1  Choose Services > Mobility Services.
Step 2  Click the device name of the mobility services engine that you want to edit.
Step 3  From the left sidebar menu, choose Systems > Accounts > Groups.
Step 4  Click the group name of the group that you want to edit.
Step 5  Choose a permission level from the Permission drop-down list.
Step 6  Click Save to apply your change.

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 mobility services engine settings.

Monitoring Status Information for a Mobility Services Engine

The System > Status page enables you to monitor server events, Prime Infrastructure alarms and events, and NMSP connection status for the mobility services engine.
Viewing Server Events for a Mobility Services Engine

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

- **Step 1** Choose **Services > Mobility Services**.
- **Step 2** Click the name of the applicable mobility services engine.
- **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.

Viewing Audit Logs from a Mobility Services Engine

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

- **Step 1** Choose **Services > Mobility Services**.
- **Step 2** Click the name of the applicable mobility services engine.
- **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.

Viewing Prime Infrastructure Alarms for a Mobility Services Engine

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

- **Step 1** Choose **Services > Mobility Services**.
- **Step 2** Click the name of the applicable mobility service.
- **Step 3** From the left sidebar menu, choose **System > Status > Prime Infrastructure Alarms**. See the “Monitoring Alarms” section on page 5-128 for more information.
Viewing Prime Infrastructure Events for a Mobility Services Engine

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

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

**Step 2** Click the name of the applicable mobility service.

**Step 3** From the left sidebar menu, choose **System > Status > Prime Infrastructure Events**. See the “Monitoring Events” section on page 5-143 for more information.

Viewing NMSP Connection Status for a Mobility Services Engine

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

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

To verify the NMSP connection between the controller and the mobility services engine, follow these steps:

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

**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 “Viewing NMSP Connection Status Details” section on page 16-759 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 mobility services engine.
Viewing NMSP Connection Status Details

To view NMSP Connection Status details, follow these steps:

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

**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 mobility services engine.
  - 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.
Managing Maintenance for Mobility Services

Viewing or Editing Mobility Services Backup Parameters

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Services &gt; Mobility Services.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the name of the mobility service whose properties you want to edit.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose Maintenance &gt; Backup.</td>
</tr>
<tr>
<td></td>
<td>• Backups located at—Indicates the location of the backup file.</td>
</tr>
<tr>
<td></td>
<td>• Enter a name for the Backup—Enter or edit the name of the backup file.</td>
</tr>
<tr>
<td></td>
<td>• Timeout (in secs)—Indicates the length of time (in seconds) before attempts to back up files times out.</td>
</tr>
</tbody>
</table>

Backing Up Mobility Services Engine Historical Data

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

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Prime Infrastructure UI, choose Services &gt; Mobility Services.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the name of the mobility services engine that you want to back up.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose Maintenance &gt; Backup.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the name of the backup.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter the time in seconds after which the backup times out.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Submit to back up the historical data to the hard drive of the server running Prime Infrastructure.</td>
</tr>
</tbody>
</table>

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.

Note You can run the backup process in the background while working on other mobility services engine operations in another Prime Infrastructure page.
Restoring Mobility Services Engine Historical Data

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

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

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

**Step 3** From the left sidebar menu, choose 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 mobility services engine.

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

**Step 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, the Prime Infrastructure shows a message to that effect.

---

Downloading Software to a Mobility Services Engine Using the Prime Infrastructure

To download software to a mobility services engine using the Prime Infrastructure, follow these steps:

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

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

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

**Step 4** On the left sidebar menu, choose Maintenance.

**Step 5** Click Download Software.

To download software, do one of the following:

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

---

### Configuring Partner System for a Mobility Services Engine

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.

### Qualcomm PDS Configuration

To configure Qualcomm PDS for MSE, follow these steps:

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

**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 to 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](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.

MSE-Qualcomm Configuration

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

Generating Map Extraction Tool (MET) Output from CAD File

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 the 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 on any host machine. Only the output of MET is used as MAP related input information on the Prime Infrastructure.

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.

Managing Cisco Adaptive wIPS Service Parameters

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.

Managing wIPS Service Administration Settings

To view or manage wIPS service administration settings, follow these steps:
Step 1  Choose Services > Mobility Services Engines.

Step 2  Choose the device name of the applicable mobility services engine.

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.

Managing Context-Aware Service Software Parameters

Context-Aware Service (CAS) software allows a mobility services engine 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.

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

Note 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.

Viewing Contextual Information

Before you can use the Prime Infrastructure to view contextual information, initial configuration for the mobility services engine is required using a command-line interface (CLI) console session. See the Cisco 3355 Mobility Services Engine Getting Started Guide and the Cisco 3100 Mobility Services Engine Getting Started Guide at the following URL:


After its installation and initial configuration are complete, the mobility services engine can communicate with multiple Cisco wireless LAN controllers to collect operator-defined contextual information. You can then use the associated Prime Infrastructure to communicate with each mobility services engine to transfer and display selected data.
You can configure the mobility services engine to collect data for clients, rogue access points, rogue clients, mobile stations, interferers, and active RFID asset tags.

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


For additional information on Context-Aware parameters, see the following topics:

- Context-Aware Service General Parameters, page 16-765
- Context-Aware Service Administration Parameters, page 16-766
- Context-Aware Service Advanced Parameters, page 16-784

Context-Aware Service General Parameters

To access the Context Aware Service > General page, choose Services > Mobility Services Engines> 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
Context-Aware Service Administration Parameters

Modifying Tracking Parameters for Mobility Services

The mobility services engine 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 mobility services engine from the Cisco wireless LAN controller.

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

You can modify the following tracking parameters using the 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 a mobility services engine, follow these steps:

Step 1  Choose Services > Mobility Services Engines to open the Mobility Services page.
Step 2  Click the name of the mobility services engine whose properties you want to edit. The General Properties page appears.
Step 3  Choose Context-Aware Software > Tracking Parameters from the Administration subheading to display the configuration options.
Step 4  Modify the following tracking parameters as appropriate (see Table 16-4).
Table 16-4  Tracking Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking Parameters</td>
<td></td>
</tr>
<tr>
<td>Wired Clients</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of client stations by the mobility services engine. 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 mobility services engine 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> When upgrading the mobility services engine 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.</td>
</tr>
<tr>
<td></td>
<td>Note Active Value (Display only): Indicates the number of wired client stations currently being tracked.</td>
</tr>
<tr>
<td></td>
<td>Note Not Tracked (Display only): Indicates the number of wired client stations beyond the limit.</td>
</tr>
<tr>
<td>Wireless Clients</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of client stations by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Enable Limiting</strong> check box to set a limit on the number of client stations to track.</td>
</tr>
<tr>
<td></td>
<td>3. 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 a mobility services engine.</td>
</tr>
<tr>
<td></td>
<td>Note The actual number of tracked clients is determined by the license purchased.</td>
</tr>
<tr>
<td></td>
<td>Note Active Value (Display only): Indicates the number of client stations currently being tracked.</td>
</tr>
<tr>
<td></td>
<td>Note Not Tracked (Display only): Indicates the number of client stations beyond the limit.</td>
</tr>
</tbody>
</table>
Table 16-4  Tracking Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue Access Points</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of rogue clients and asset points by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Enable Limiting</strong> check box to set a limit on the number of rogue clients and asset tags stations to track.</td>
</tr>
<tr>
<td></td>
<td>3. 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 a mobility services engine.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (Display only): Indicates the number of rogue clients and access points currently being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (Display only): Indicates the number of rogue clients beyond the limit.</td>
</tr>
<tr>
<td>Exclude Ad-Hoc Rogues</td>
<td>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 the Prime Infrastructure maps or its events and alarms reported.</td>
</tr>
<tr>
<td>Rogue Clients</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of rogue clients by the mobility services engine.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Enable Limiting</strong> check box to set a limit on the number of rogue clients to track.</td>
</tr>
<tr>
<td></td>
<td>3. 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 a mobility services engine.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (Display only): Indicates the number of rogue clients being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (Display only): Indicates the number of rogue clients beyond the limit.</td>
</tr>
</tbody>
</table>
**Table 16-4  Tracking Parameters (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interferers</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of the interferers by the mobility services engine. 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (Display only): Indicates the number of interferers currently being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (Display only): Indicates the number of interferers beyond the limit.</td>
</tr>
</tbody>
</table>

**Asset Tracking Elements**

| Active RFID Tags          | 1. Select the **Enable** check box to enable tracking of active RFID tags by the mobility services engine. |
|                          | **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.

<table>
<thead>
<tr>
<th>SNMP Retry Count</th>
<th>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.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Timeout</td>
<td>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.)</td>
</tr>
</tbody>
</table>

**SNMP Polling Interval**

<table>
<thead>
<tr>
<th>Client Stations</th>
<th>Select the <strong>Enable</strong> 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.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active RFID Tags</td>
<td>Select the <strong>Enable</strong> check box to enable active RFID tag polling and enter the polling interval in seconds. Allowed values are from 1 to 99999.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Before the mobility service can collect asset tag data from controllers, you must enable the detection of active RFID tags using the <strong>config rfid status enable</strong> CLI command on the controllers.</td>
</tr>
<tr>
<td>Rogue Clients and Access Points</td>
<td>Select the <strong>Enable</strong> 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.)</td>
</tr>
<tr>
<td>Statistics</td>
<td>Select the <strong>Enable</strong> 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.)</td>
</tr>
</tbody>
</table>
Step 5  Click **Save** to store the new settings in the mobility services engine database.

**Filtering Parameters for Mobility Services**

In the Prime Infrastructure, 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 Table 16-5 for details.

  **EXAMPLE** file listing:

  ```
  [Allowed]
  00:11:22:33:*
  22:cd:34:ae:56:45
  02:23:34:34:*
  [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.

**Modifying Filtering Parameters**

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

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

**Step 2**  Click the name of the mobility services engine whose properties you want to edit. The General Properties page appears.

**Step 3**  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 Table 16-5).
### Table 16-5  Filtering Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Filtering Params</td>
<td></td>
</tr>
</tbody>
</table>
| 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 Params       |                                                                                                                                                       |
Table 16-5 Filtering Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude Probing Clients</td>
<td>Select the check box to prevent location calculation of probing clients.</td>
</tr>
</tbody>
</table>
| Enable Location MAC Filtering| 1. Select the check box to enable MAC filtering of specific elements by their MAC address.  
|                              | 2. 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. |
|                              | 3. 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 mobility services engine database.
Modifying History Parameters for Mobility Services

You can use the 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:

Step 1 Choose Services > Mobility Services.
Step 2 Click the name of the mobility service whose properties you want to edit.
Step 3 From the left sidebar menu, choose Context Aware Service > History Parameters.
Step 4 Modify the following history parameters as appropriate (see Table 16-6).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive for</td>
<td>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.</td>
</tr>
<tr>
<td>Prune data starting at</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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.
Enabling Location Presence for Mobility Services

You can enable location presence on the mobility services engine 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 mobility services engine is capable of providing any requesting Cisco CX v5 client its location.

Note  
Before enabling this feature, synchronize the mobility services engine.

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

Step 1  Choose Services > Mobility Services > Device Name. Select the mobility services engine to which the campus or building or floor is assigned.

Step 2  From the left sidebar menu, choose Context Aware Services > Administration > Presence Parameters.

Step 3  Select the Service Type On Demand check box to enable location presence for Cisco CX clients v5.

Step 4  Select one of the following Location Resolution options:

a. When Building is selected, the mobility services engine can provide any requesting client, its location by building.
   – For example, if a client requests its location and the client is located in Building A, the mobility services engine returns the client address as Building A.

b. When AP is selected, the mobility services engine can provide any requesting client, its location by its associated access point. The MAC address of the access point appears.
   – For example, if a client requests its location and the client is associated with an access point with a MAC address of 3034:00hh:0adg, the mobility services engine returns the client address of 3034:00hh:0adg.

c. When X,Y is selected, the mobility services engine can provide any requesting client, its location by its X and Y coordinates.
   – For example, if a client requests its location and the client is located at (50, 200) the mobility services engine returns the client address of 50, 200.

Step 5  Select any or all of the location formats:

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.

Note  
See the “Importing Civic Information for Mobility Services” section on page 16-776 for more information on importing a file with multiple Civic listings.
Step 6  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 7  Select the Retransmission Rule check box to allow the receiving client to retransmit the received information to another party.

Step 8  Enter a Retention Expiration value in minutes. This determines how long the received information is stored by the client before it is overwritten. The default value is 24 hours (1440 minutes).

Step 9  Click Save.

**Importing Asset Information for Mobility Services**

To import asset, chokepoint, and TDOA receiver information for the mobility services engine using the Prime Infrastructure, follow these steps:

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

**Step 2**  Click the name of the mobility services engine for which you want to import information.

**Step 3**  Choose Context Aware Service > Administration > Import Asset Information.

**Step 4**  Enter the name of the text file or browse for the filename.

Specify information in the imported file in the following formats:

- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

**Step 5**  When the import filename is located in the Browse text box, click Import.

**Exporting Asset Information for Mobility Services**

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

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

**Step 2**  Click the name of the mobility services engine from which you want the export information.

**Step 3**  Choose Context Aware Service > Administration > Export Asset Information.

Information in the exported file is in the following formats:

- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

**Step 4**  Click Export.

Click Open (display to screen), Save (to external PC or server), or Cancel (to cancel the request).
Chapter 16  Prime Infrastructure Services

Mobility Services

**Note**  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.

---

**Importing Civic Information for Mobility Services**

To import civic information for the mobility services engine using the Prime Infrastructure, follow these steps:

1. **Step 1**  Choose Services > Mobility Services.
2. **Step 2**  Click the name of the mobility services engine for which you want to import asset information.
3. **Step 3**  From the left sidebar menu, choose Context Aware Software.
4. **Step 4**  From the Administration left sidebar menu, choose Import Civic Information.
5. **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”
   
   **Note**  Each entry must appear on a separate line.
6. **Step 6**  Click Import.

---

**Context-Aware Service Wired Parameters**

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

**Monitoring Wired Switches**

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 mobility services engine through the Prime Infrastructure when the Ethernet switch and the mobility services engine are synchronized (Services > Synchronize Services > Switches). Communication between a location-capable switch and the mobility services engine is over NMSP. The Prime Infrastructure and the mobility services engine communicate over XML.

To view details on wired switches, follow these steps:

1. **Step 1**  Choose Services > Mobility Services.
2. **Step 2**  In the Mobility Services page, click the device name link of the appropriate wired location switch.
3. **Step 3**  Choose Context Aware Service > Wired > Wired Switches. A summary of wired switches that are synchronized with the mobility services engine appears.
**Step 4** See the “Wired Switch Details” section on page 16-777 for more information on the switch, its port, its wired clients (count and status), and its civic information click the IP address link.

---

**Wired Switch Details**

To view wired switch details, follow these steps:

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

**Step 2** In the Mobility Services page, click the device name link of the appropriate mobility services engine.

**Step 3** Choose Context Aware Service > Wired > Wired Switches. A summary of wired switches that are synchronized with the mobility services engine appears.

**Step 4** 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.

*Note* You can export civic information from the switch by choosing that option from the Select a command drop-down list. This option is available 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.

*Note* You can view detailed wired client information by clicking in one of the client count links (total clients, connected, disconnected, and unknown). See the “Monitoring Wired Clients” section on page 16-777 section for more information.

- **Switch Ports**—Displays a detailed list of the ports on the switch.

*Note* 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.

---

**Monitoring Wired Clients**

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.
Wireless client data is downloaded to the mobility services engine through the Prime Infrastructure when the switch and the mobility services engine are synchronized (Services > Synchronize Services > Switches).

The Prime Infrastructure and the mobility services engine communicate over XML.

You can view the details of the wireless client on either the wireless switches page (Context Aware Service > Wired > Wireless Switches) or wireless clients page (Context Aware Service > Wired > Wireless Clients).

- If you know the IP address, MAC address, VLAN ID, serial number, or username, you can use the search field on the wireless clients page.
- If you want to examine wireless clients as they relate to a specific switch, you can view that information on the wireless switches page. See the “Monitoring Wireless Switches” section on page 16-776 for more information.

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

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

**Step 2** Click the device name link of the appropriate wireless location switch.

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

In the Wireless 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 wireless switch.
- Disconnected clients—Clients that are disconnected from the wireless switch.
- Unknown clients—Clients that are marked as unknown when the NMSP connection to the wireless switch is lost. See the “Viewing NMSP Connection Status for a Mobility Services Engine” section on page 16-758 for more information about NMSP connections.

If you know the MAC address of the wireless client, you can click that link to reach the detail page of the client or use the search field. See the “Wireless Client Details” section on page 16-778 for more information on wireless client details.

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

If you click the IP address of the switch, you are forwarded to the detail page of the switch. See the “Monitoring Wireless Switches” section on page 16-776 for more information.

**Step 4** Click the MAC Address for the applicable client to view wireless client details. See the “Wireless Client Details” section on page 16-778 for more information on wireless client details.

---

**Wireless Client Details**

To view wireless client details, follow these steps:

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

**Step 2** In the Mobility Services page, click the device name link of the appropriate mobility services engine.

**Step 3** Choose Context Aware Service > Wired > Wireless Clients. A summary of wireless clients that are synchronized with the mobility services engine appears.

**Step 4** Click the MAC address link for the applicable wireless client. The Wireless 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.

**Note**

A client takes on the civic address and advanced location information that is configured for the port on which the client terminates. If no civic and advanced information is defined for the its port (port/slot/module) then no location data is displayed.

---

### Monitoring Interferers

The Monitor > Interferers page allows you to monitor interference devices detected by the CleanAir-enabled access points.

This section provides information on the interferers detected by the CleanAir-enabled access points. By default, the **Monitor > Interferers > AP Detected Interferers**, page 16-779 page is displayed.

**Monitor > Interferers > AP Detected Interferers**

Choose **Monitor > Interferers** to view all the interfering devices detected by the CleanAir-enabled access points on your wireless network. This page enables you to view a summary of the interfering devices including the following default information:

- **Interferer ID**—A unique identifier for the interferer. Click this link to know more about the interferer.
- **Type**—Indicates the category of the interferer. Click to read more about the type of device. The dialog box appears displaying more details. The categories include the following:
  - Bluetooth link—A Bluetooth link (802.11b/g/n only)
  - Microwave Owen—A microwave oven (802.11b/g/n only)
  - 802.11 FH—An 802.11 frequency-hopping device (802.11b/g/n only)
  - Bluetooth Discovery—A Bluetooth discovery (802.11b/g/n only)
  - TDD Transmitter—A time division duplex (TDD) transmitter
  - Jammer—A jamming device
  - Continuous Transmitter—A continuous transmitter
  - DECT-like Phone—A digital enhanced cordless communication (DECT)-compatible phone
  - Video—A video camera
  - 802.15.4—An 802.15.4 device (802.11b/g/n only)
  - WiFi Inverted—A device using spectrally inverted Wi-Fi signals
- WiFi Invalid—A device using non-standard Wi-Fi channels
- SuperAG—An 802.11 SuperAG device
- Canopy—A Motorola Canopy device
- Radar—A radar device (802.11a/n only)
- XBox—A Microsoft Xbox (802.11b/g/n only)
- WiMAX Mobile—A WiMAX mobile device (802.11a/n only)
- WiMAX Fixed—A WiMAX fixed device (802.11a/n only)
- TDD Exalt
- Motorola Canopy

- Status—Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir-enabled access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir-enabled access point or the CleanAir-enabled access point determined that the interferer is no longer reachable by the Prime Infrastructure.

- Severity—Displays the severity ranking of the interfering device.

- Affected Band—Displays the band in which this device is interfering.

- Affected Channels—Displays the affected channels.

- Duty Cycle (%)—The duty cycle of interfering device in percentage.

- Discovered—Displays the time at which it was discovered.

- Last Updated—The last time the interference was detected.

- Floor—The location where the interfering device is present.

---

**Note**

These devices appear only if the option to track Interferers is enabled in the Tracking Parameters page. This option is disabled by default. See the “Modifying Tracking Parameters for Mobility Services” section on page 16-766 for more information on tracking parameters.

---

**Monitor > Interferers > AP Detected Interferers > Interferer Details**

Choose **Monitor > Interferers > Interferer ID** to view this page. This page enables you to view the details of the interfering devices detected by the access points. This page provides the following details about the interfering device.

- Interferer Properties
  - Type—Displays the type of the interfering device detected by the AP.

- Status—The status of the interfering device. Indicates the status of the interfering device.
  - Active—Indicates that the interferer is currently being detected by the CleanAir-enabled access point.
  - Inactive—Indicates that the interferer is no longer being detected by the CleanAir-enabled access point or the CleanAir-enabled access point saw the interferer no longer reachable by the Prime Infrastructure.

- Severity—Displays the severity ranking of the interfering device.
– Duty Cycle (%)—The duty cycle of interfering device in percentage.
– Affected Band—Displays the band in which this device is interfering.
– Affected Channels—Displays the affected channels.
– Discovered—Displays the time at which it was discovered.
– Last Updated—The last time the interference was detected.

• Location
  – Floor—The location where this interfering device was detected.
  – Last Located At—The last time where the interfering device was located.
  – On MSE—The Mobility Server Engine on which this interference device was located.

• Clustering Information
  – Clustered By—Displays the following:
    IP address of the controller if clustered by a controller.
    IP address of the mobility services engine if clustered by a mobility services engine.
  – Detecting APs—Displays the details of the access point that has detected the interfering device.
    The details include: Access Point Name (Mac), Severity, and Duty Cycle(%).

Note
The detecting access point information is available only for active devices. And even for some active devices, this information might not be available. This is because these interferers are in the process of being marked inactive and in the next refresh of Monitor > Interferers page, these appear as inactive.

• Details—Displays a short description about the interfering type.

Select a command
The Select a command drop-down list provides access to the location history of the interfering device detected by the access point. See the “Monitor > Interferers > AP Detected Interferer Details > Interference Device ID > Location History” section on page 16-781 for more information.

Monitor > Interferers > AP Detected Interferer Details > Interference Device ID > Location History

Choose Monitor > Interferers > Interference Device ID, choose Location History from the Select a command drop-down list, and click Go to view this page.

• Interferer Information—Displays the basic information about the interfering device.
  – Data Collected At—The time stamp at which the data was collected.
  – Type—The type of the interfering device.
  – Severity—The severity index of the interfering device.
  – Duty Cycle—The duty cycle (in percentage) of the interfering device.
  – Affected Channels—A comma separated list of the channels affected.

• Interferer Location History—Displays the location history of the interfering devices.
  – Time Stamp
  – Floor

• Clustering Information
- Clustered By
- Detecting APs
  - AP Name—The access point that detected the interfering device.
  - Severity—The severity index of the interfering device.
  - Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.
- Location
  - Location Calculated At—Displays the time stamp at which this information was generated.
  - Floor—Displays location information of the interfering device.
  - A graphical view of the location of the interfering device is displayed in a map. Click the Enlarge link to view an enlarged image.

**Monitor > Interferers > Edit View**

The Edit View page allows you to add, remove, or reorder columns in the AP Detected Interferers Summary page. It also allows you to search for Interferers. By default, only those interferers that are in Active state and with a severity greater than or equal to 5 are displayed in the AP Detected Interferers page. See the “Monitor > Interferers > Edit View > Edit Search” section on page 16-782 for more information on editing search criteria.

To edit the columns in the AP Detected Interferers page, follow these steps:

**Step 1** Choose Monitor > Interferers. The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir-enabled access points.

**Step 2** Click the Edit View link in the AP Detected Interferers page.

**Step 3** To add an additional column to the access points table, click to highlight the column heading in the left column. Click Show to move the heading to the right column. All items in the right column are displayed in the table.

**Step 4** To remove a column from the access points table, click to highlight the column heading in the right column. Click Hide to move the heading to the left column. All items in the left column are not displayed in the table.

**Step 5** Use the Up/Down buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click Up or Down to move it higher or lower in the current list.

**Step 6** Click Reset to restore the default view.

**Step 7** Click Submit to confirm the changes.

**Monitor > Interferers > Edit View > Edit Search**

You can search for interferers based on certain criteria. By default only those interferers that are in Active state and with severity greater than or equal to 5 are displayed in the AP Detected Interferers page. Use the Edit Search option to customize the interferer search.

To edit the search criteria, follow these steps:

**Step 1** Choose Monitor > Interferers. The AP Detected Interferers page appears.
Step 2  Click **Edit Search** and select the appropriate criteria. This option allows you to specify the following search criteria:

- **Search Category**—For interferer search, the search category is Interferers.
- **Detected By**—From the drop-down list, choose **Access Points** or **Spectrum Experts**.
- **Search By**—From the drop-down list, choose any one of the following options:
  - All Interferers
  - Interferer ID
  - Interferer Type
  - Severity
  - Duty Cycle
  - Location
- **Severity greater than**—Enter the severity level in the text box.
- **Detected within the last**—From the drop-down list, choose any one of the following options:
  - 5 Minutes
  - 15 Minutes
  - 30 Minutes
  - 1 Hour
  - 3 Hours
  - 6 Hours
  - 12 Hours
  - 24 Hours
  - All History
- **Interferer status**—From the list, choose any of the following options:
  - Active
  - Inactive
  - All
- **Restrict By Radio Band/Channels**—Select this check box if you want to restrict certain radio frequencies or channels from the search. By default, this check box is unselected. On selection of this check box, a list appears with 2.4-GHz, 5-GHz and Individual Channel options. If you select Individual Channel, an Affected Channels text box appears. Specify the channel and select either the **Match All** or **Match Any** radio button.

Step 3  Select the number of items per page that you want to view in the search results.

Step 4  Select the **Save Search** check box if you want to save the search.

Step 5  After specifying the search criteria, click **Go** to view the search results.
Context-Aware Service Advanced Parameters

Modifying Northbound Notifications

Northbound notifications define which tag notifications the mobility services engine sends to third-party applications.

To configure northbound parameters, follow these steps:

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

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

**Step 3** Choose Context Aware Service > Advanced > Notification Parameters to display the configuration options.

**Step 4** Select the Enable Northbound Notifications check box to enable the function.

**Step 5** Select the Notification Contents check box to send notifications to third-party applications (northbound).

**Step 6** Select one or more of the following Notification Contents check boxes:
- Chokepoints
- Telemetry
- Emergency
- Battery Level
- Vendor Data
- Location

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

**Step 8** Select one or more of the following Notification Triggers check boxes:
- Chokepoints
- Telemetry
- Emergency
- Battery Level
- Vendor Data
- Location Recalculation

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

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

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

**Step 12** To modify the notification parameter settings, enter the new value in the appropriate text box in the Advanced tab of this page. See Table 16-9.
Modifying Location Parameters for Mobility Services

You can use the 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:

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

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

**Step 3** From the left sidebar menu, choose **Context Aware Service > Location Parameters**.

**Step 4** Modify the location parameters as appropriate (see Table 16-8).

---

**Table 16-7 User-Configurable Conditional and Northbound Notifications Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limit</td>
<td>Enter the rate, in milliseconds, at which the mobility services engine generates notifications. A value of 0 (default) means that the mobility services engine generates notifications as fast as possible (Northbound notifications only).</td>
</tr>
<tr>
<td>Queue Limit</td>
<td>Enter the event queue limit for sending notifications. The mobility services engine drops any event above this limit.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>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. <strong>Note</strong> The mobility services engine does not store events in its database.</td>
</tr>
<tr>
<td>Refresh Time</td>
<td>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.</td>
</tr>
<tr>
<td>Drop Oldest Entry on Queue Overflow</td>
<td>(Read-only). The number of event notifications dropped from the queue since startup.</td>
</tr>
<tr>
<td>Serialize Events per Mac address per Destination</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Step 13** Click **Save**.
### Table 16-8 Location Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Calculation Time</td>
<td>Select the check box to enable the calculation of the time required to compute location.</td>
</tr>
<tr>
<td><img src="http://example.com" alt="Caution" /></td>
<td>Enable only under Cisco TAC personnel guidance because enabling this field slows down overall location calculations.</td>
</tr>
<tr>
<td>Enable OW Location</td>
<td>Select the check box to enable Outer Wall (OW) calculation as part of location calculation.</td>
</tr>
<tr>
<td><img src="http://example.com" alt="Note" /></td>
<td>The OW Location parameter is ignored by the location server.</td>
</tr>
<tr>
<td>Relative discard RSSI time</td>
<td>Enter the number of minutes since the most recent RSSI sample after which RSSI measurement should be considered stale and discarded. Default value is 3. Allowed values range from 0 to 99999. A value of less than 3 is not recommended.</td>
</tr>
<tr>
<td>Absolute discard RSSI time</td>
<td>Enter the number of minutes after which RSSI measurement should be considered stale and discarded, regardless of the most recent sample. Default value is 60. Allowed values range from 0 to 99999. A value of less than 60 is not recommended.</td>
</tr>
<tr>
<td>RSSI Cutoff</td>
<td>Enter the RSSI cutoff value, in decibels (dBs) with respect to one (1) mW (dBm), preceding which the mobility service always use the access point measurement. Default value is -75.</td>
</tr>
<tr>
<td><img src="http://example.com" alt="Note" /></td>
<td>When 3 or more measurements are available preceding the RSSI cutoff value, the mobility service discards any weaker values and use the 3 (or more) strongest measurements for calculation; however, when only weak measurements following the RSSI cutoff value are available, those values are used for calculation.</td>
</tr>
<tr>
<td><img src="http://example.com" alt="Caution" /></td>
<td>Modify only under Cisco TAC personnel guidance. Modifying this value can reduce the accuracy of location calculation.</td>
</tr>
</tbody>
</table>
Enable Location Filtering

If enabled, the location filter is applied only for client location calculation. Enabling location filter allows previous location estimates to be used in estimating current location. This reduces location jitter for stationary clients and improve tracking for mobile clients.

Chokepoint Usage

Select the check box to enable the usage of chokepoint proximity to determine location. Applies to Cisco-compatible Tags capable of reporting chokepoint proximity.

Use Chokepoints for Interfloor conflicts

Allows the use of chokepoints to determine the correct floor during Interfloor conflicts. Choose Never, Always, or Floor Ambiguity.

Chokepoint Out of Range Timeout

After a Cisco-compatible Tag leaves a chokepoint proximity range, this is the timeout (in seconds) after which RSSI information is used again to determine location.

Absent Data Cleanup Interval

Enter the interval period (in minutes) for removing inactive elements from the database.

Use Default Heatmaps for Non Cisco Antennas

Select this check box to enable the usage of default heatmaps for non-Cisco antennas during the Location Calculation. This option is disabled by default.

Table 16-8 Location Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Location Filtering</td>
<td>If enabled, the location filter is applied only for client location calculation.</td>
</tr>
<tr>
<td></td>
<td>Enabling location filter allows previous location estimates to be used in estimating current location.</td>
</tr>
<tr>
<td></td>
<td>This reduces location jitter for stationary clients and improve tracking for mobile clients.</td>
</tr>
<tr>
<td>Chokepoint Usage</td>
<td>Select the check box to enable the usage of chokepoint proximity to determine location.</td>
</tr>
<tr>
<td></td>
<td>Applies to Cisco-compatible Tags capable of reporting chokepoint proximity.</td>
</tr>
<tr>
<td>Use Chokepoints for Interfloor conflicts</td>
<td>Allows the use of chokepoints to determine the correct floor during Interfloor conflicts.</td>
</tr>
<tr>
<td></td>
<td>Choose Never, Always, or Floor Ambiguity.</td>
</tr>
<tr>
<td>Chokepoint Out of Range Timeout</td>
<td>After a Cisco-compatible Tag leaves a chokepoint proximity range, this is the timeout (in seconds)</td>
</tr>
<tr>
<td></td>
<td>after which RSSI information is used again to determine location.</td>
</tr>
<tr>
<td>Absent Data Cleanup Interval</td>
<td>Enter the interval period (in minutes) for removing inactive elements from the database.</td>
</tr>
<tr>
<td>Use Default Heatmaps for Non Cisco Antennas</td>
<td>Select this check box to enable the usage of default heatmaps for non-Cisco antennas during the</td>
</tr>
<tr>
<td></td>
<td>Location Calculation. This option is disabled by default.</td>
</tr>
<tr>
<td>Movement Detection</td>
<td>This field specifies the Individual RSSI movement recalculation trigger threshold.</td>
</tr>
<tr>
<td>Individual RSSI change threshold</td>
<td>Enter a threshold value between 0-127 dBm.</td>
</tr>
<tr>
<td></td>
<td>Do not modify without Cisco TAC guidance.</td>
</tr>
<tr>
<td>Aggregated RSSI change threshold</td>
<td>This field specifies the Aggregated RSSI movement recalculation trigger threshold.</td>
</tr>
<tr>
<td></td>
<td>Enter a threshold value between 0-127 dBm.</td>
</tr>
<tr>
<td></td>
<td>It should not be modified without Cisco TAC guidance.</td>
</tr>
<tr>
<td>Many new RSSI change percentage threshold</td>
<td>This field specifies Many new RSSI movement recalculation trigger threshold in percentage.</td>
</tr>
<tr>
<td></td>
<td>It should not be modified without Cisco TAC guidance.</td>
</tr>
<tr>
<td>Many missing RSSI percentage threshold</td>
<td>This field specifies Many missing RSSI movement recalculation trigger threshold in percentage.</td>
</tr>
<tr>
<td></td>
<td>It should not be modified without Cisco TAC guidance.</td>
</tr>
</tbody>
</table>
Step 5  Click **Save** to store your selections in the Prime Infrastructure and mobility service databases.

---

**Modifying Notification Parameters for Mobility Services**

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

**Note**  Modify notification parameters only if you expect the mobility services engine 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 mobility services engine is available on the Cisco developers support portal at the following URL:


To configure notification parameters, follow these steps:

---

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

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

**Step 3**  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 following Notification content options:

* Chokepoints
* Telemetry
* Emergency
* Battery Level
* Vendor Data
* Location

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

**Step 8**  Select one or more of the following Notification trigger options:

* Chokepoints
* Telemetry
* Emergency
* Battery Level
* Vendor Data
* Location Recalculation

**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. Table 16-9 describes each parameter.

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limit</td>
<td>Enter the rate in milliseconds at which the mobility services engine generates notifications. A value of 0 (default) means that the mobility services engine generates notifications as fast as possible (Northbound notifications only).</td>
</tr>
<tr>
<td>Queue Limit</td>
<td>Enter the event queue limit for sending notifications. The mobility services engine drops any event preceding this limit.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the number of times to generate an event notification before the refresh time expires. This field can be used for asynchronous transport types which do not acknowledge the receipt of the notification and there is a possibility that the notification might be lost in transit. Default value is 1.</td>
</tr>
<tr>
<td>Note</td>
<td>The mobility services engine does not store events in its database.</td>
</tr>
<tr>
<td>Refresh Time</td>
<td>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.</td>
</tr>
<tr>
<td>Drop Oldest Entry on Queue Overflow</td>
<td>(Read-only). The number of event notifications dropped from the queue since startup.</td>
</tr>
<tr>
<td>Serialize Events per Mac address per Destination</td>
<td>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.</td>
</tr>
</tbody>
</table>

Step 13  Click Save.

Viewing Partner Engine Status

To access the Partner Engine Status page, choose Services > Mobility Services > 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.

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

Table 16-10 describes the fields in the Tag Engine Status page for the Aeroscout Tag Engine.
Chapter 16  Prime Infrastructure Services

Mobility Services

Table 16-10  Partner Engine Status Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner Location Engine Name</td>
<td>The Partner engine name, which is aeroscout.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the Aeroscout Tag Engine.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the Tag Engine.</td>
</tr>
<tr>
<td>Registered</td>
<td>Appears as True when the Aeroscout Tag Engine has established communication with the mobility services engine.</td>
</tr>
<tr>
<td>Active</td>
<td>Appears as True when the Aeroscout Tag Engine is up and running.</td>
</tr>
<tr>
<td>License Information</td>
<td>The maximum tags that are available with the Aeroscout Tag Engine.</td>
</tr>
</tbody>
</table>

If you selected Cisco Tag Engine for Context Aware Service, the Tag Engine Status page displays the following information.

Table 16-11 describes the fields in the Tag Engine Status page for the Cisco Tag Engine.

Table 16-11  Tag Engine Status Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag Location Engine Name</td>
<td>The Tag location engine name, which is Cisco.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the Cisco Tag Engine.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the Cisco Tag Engine.</td>
</tr>
<tr>
<td>Active</td>
<td>Displays as True when the Cisco Tag Engine is up and running.</td>
</tr>
<tr>
<td>License Information</td>
<td>The maximum tags that are available with the Cisco Tag Engine.</td>
</tr>
</tbody>
</table>

Viewing Notification Information for Mobility Services

The Services > Context Aware Notifications page provides the ability to define events.

Viewing the Notifications Summary for Mobility Services

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

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

- Absence (Missing)—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.

Note: You define a containment area (campus, building, or floor) in the Maps section of the Prime Infrastructure (Monitor > Maps). 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

Note: 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.

Notifications Cleared

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

Note: In the Prime Infrastructure, the Notifications Summary page reflects whether notifications for cleared event conditions have been received.
Viewing and Managing Notifications for Mobility Services

To view the Notification Definitions, choose Services > Context Aware Notifications > Notification 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 “Adding Event Groups” section on page 16-794 and “Adding Event Definitions” section on page 16-797.

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

Table 16-13 lists and describes the fields in the Notification Definition page.

### Table 16-12 Notification Definition Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Name of the group to which the event definition is added.</td>
</tr>
<tr>
<td>Event Definitions</td>
<td>Existing event definitions for the event group.</td>
</tr>
<tr>
<td>Created On</td>
<td>Date on which the event groups are created.</td>
</tr>
</tbody>
</table>

Viewing Notification Statistics

You can view the notification statistics for a specific mobility services engine. To view the Notification Statistics for a specific mobility services engine, choose Services > Mobility Services > MSE-name > Context Aware Service > Notification Statistics.

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

Table 16-13 lists and describes the fields in the Notification statistics page.

### Table 16-13 Notification Statistics Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td></td>
</tr>
<tr>
<td>Destinations</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>Total count of the destinations.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Count of unreachable destinations.</td>
</tr>
<tr>
<td>Notification Statistics Summary</td>
<td></td>
</tr>
<tr>
<td>Track Definition Status</td>
<td>Status of the track definition. Track notification status can be either Enabled or Disabled.</td>
</tr>
<tr>
<td>Track Definition</td>
<td>Track definition can be either Northbound or CAS event notification.</td>
</tr>
<tr>
<td>Destination IP Address</td>
<td>The destination IP address to which the notifications are sent.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>The destination port to which the notifications are sent.</td>
</tr>
<tr>
<td>Destination Type</td>
<td>The type of the destination. For example, SOAP_XML.</td>
</tr>
</tbody>
</table>
Mobile Concierge Service Parameters

Viewing the Configured Service Advertisements

To view the configured service advertisements, follow these steps:

Step 1 Choose Services > Mobility Services Engine.
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.

Viewing Mobile Concierge Service Statistics

To view Mobile Concierge service statistics, follow these steps:

Step 1 Choose Services > Mobility Services Engine.
Step 2 Click Device Name to view its properties.
Step 3 Choose Mobile Concierge service > Statistics from the left sidebar menu.

Table 16-13 Notification Statistics Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Status</td>
<td>Status of the destination device. The status is either Up or Down.</td>
</tr>
<tr>
<td>Last Sent</td>
<td>The date and time at which the last notification was sent to the destination device.</td>
</tr>
<tr>
<td>Last Failed</td>
<td>The date and time at which the notification had failed.</td>
</tr>
<tr>
<td>Total Count</td>
<td>The total count of notifications sent to the destination. Click the count link to view the notification statistics details of the destination device.</td>
</tr>
</tbody>
</table>
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.

### About Event Groups

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

**Note**

For more information about synchronizing the Cisco wireless LAN controllers and the Prime Infrastructure with mobility services engines see the “Synchronizing Services” section on page 16-730.

### Adding Event Groups

To add an event group, follow these steps:

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

The new event group appears in the Event Settings page.

### Deleting Event Groups

To delete an event group, follow these steps:

1. Choose **Services > Context Aware Notifications**.
2. Choose **Notification Definitions** from the left sidebar menu.
3. Select the check box of the event group you want to delete.
4. From the Select a command drop-down list, choose **Delete Event Group(s)**.
5. Click **Go**.
6. Click **OK** to confirm the deletion.
7. Click **Save**.
Chapter 16  Prime Infrastructure Services

Mobility Services

Working with 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.

Note
The 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:

Step 1 Choose Services > Context Aware Notifications.
Step 2 From the left sidebar menu, choose Notification Definitions.
Step 3 Click the name of the group to which you want to add 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.

Note
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.

Note
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 (Table 16-14).
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.

Note Emergency and chokepoint events are only applicable to tags (CCXv.1 compliant).

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), and enter the relevant text for the selected Match By element.

e. 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.

Table 16-14 Condition Type/Trigger If Parameters

<table>
<thead>
<tr>
<th>Condition Type</th>
<th>Trigger If</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing</td>
<td>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 mobility services engine generates a missing asset event if the mobility services engine has not located the asset for more than 10 minutes.</td>
</tr>
<tr>
<td>In/Out</td>
<td>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).</td>
</tr>
<tr>
<td>Distance</td>
<td>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.</td>
</tr>
<tr>
<td>Battery Level</td>
<td>Battery Level Is—Low, Medium, Normal. Select the appropriate battery level that triggers an event.</td>
</tr>
<tr>
<td>Location Change</td>
<td>An event is triggered if the location of the asset changes.</td>
</tr>
<tr>
<td>Emergency</td>
<td>Select Any, Panic Button, Tampered, or Detached check box.</td>
</tr>
<tr>
<td>Chokepoint</td>
<td>In the range of Chokepoints—Click Select Chokepoint check box and choose the chokepoint parameters in the Select page. Click Select.</td>
</tr>
</tbody>
</table>
The recipient system must have an event listener running to process notifications. By default, when you create an event definition, the Prime Infrastructure adds its IP address as the destination.

c. 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.

d. From the Message Format field drop-down list, select XML or Plain Text.

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

e. 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.

f. Click Add.

Step 11 Verify that the new event definition is listed for the event group (Context Aware Service > Notifications > Event > Settings > Event Group Name).

Adding Event Definitions

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

The 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:

**Step 1**  Choose **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.

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

   If you chose Battery Level from the Condition Type drop-down list, select the check box next to the 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.

Note 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.

Note 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.

Note 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.

The recipient system must have an event listener running to process notifications. By default, when you create an event definition, the Prime Infrastructure adds its IP address as the destination.

d. 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.
Chapter 16            Prime Infrastructure Services

Mobility Services

Choose XML or Plain Text to specify the message format.

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.

g. To enable HTTPS, select the Enable check box next to it.

  Port Number auto-populates.

h. 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.

   **Note** An event notification with high priority is serviced before event definitions with lower priority.

c. To select how often the event notifications are sent:

   1. Select the All the Time check box to continuously report events. Proceed to Step g.
   2. Unselect the All the Time check box to select the day and time of the week that you want event notifications sent. Days of the week and time fields appear for the selection. Proceed to Step d.

d. Select the check box next to each day you want the event notifications sent.

e. Select the time for starting the event notification by selecting the appropriate hour, minute, and AM/PM options from the Apply From heading.

f. Select the time for ending the event notification by selecting the appropriate hour, minute, and AM/PM options from the Apply Until heading.

g. Click Save.
Deleting an Event Definition

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

Step 1 Choose Services > Context Aware Notifications.
Step 2 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.

Client Support on MSE

You can use the Prime Infrastructure advanced search feature to narrow the client list based on specific categories and filters. You can also filter the current list using the Show drop-down list.

This section contains the following topics:

- Searching a Wireless Client from the Prime Infrastructure on the MSE by IPv6 Address, page 16-801
- Viewing the Clients Detected by the MSE, page 16-802

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

Note Only wireless clients have IPv6 addresses in this release.

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

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.

Note The Wireless Type drop-down list appears only when you choose Wireless Clients as the media type.
Step 4 From the Wireless Type drop-down list, choose any of the following types: All, Lightweight or Autonomous Clients.

Step 5 From the Search By drop-down list, choose IP Address.

**Note** Searching a client by IP address can contain either 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 either a partial or full IPv6 address.

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

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

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

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

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

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

Step 14 Select the Include Disassociated check box to include clients that are no longer on the network but for which the Prime Infrastructure has historical records.

Step 15 From the Items per page drop-down list, choose the number of records to be displayed in the search results page.

Step 16 Select the Save Search check box to save the selected search option.

Step 17 Click Go.

The Clients and Users page appears with all the clients detected by the MSE.

---

**Viewing the Clients Detected by the MSE**

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

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

The Client and Users page appears.
The Clients and Users table displays a few columns by default. If you want to display the additional columns that are available, click \( \text{Columns} \), and then click \text{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 \textit{Clients detected by MSE} from the Show drop-down list.

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

The following different parameters are available in the Clients Detected by MSE table:

- **MAC Address**—Client MAC address.
- **IP Address**—Client IP address.

The IP Address that appears in the IP Address column is determined by a predefined priority order. The first IP address available in the following order appears in the IP address text box:

- IPv4 address

\textbf{Note} Only wireless clients have IPv6 addresses in this release. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

- IPv6 global unique address. If there are multiple addresses of this type, most recent IPv6 address that the client received is shown, because a user could have two Global IPv6 addresses but one might have been from an older Router Advertisement that is being aged out.
- IPv6 local unique address. If there are multiple IPv6 local unique addresses, then the most recent address appears.
- IPv6 link local address. For an IPv6 client it always have at least a link local address.

The following are the different IPv6 address types:

- Link-local Unicast—The link-local addresses are designed to be used for addressing on a single link for purposes such as auto-address configuration, neighbor discovery, or when no routers are present.
- Site-local Unicast—The site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix.
- Aggregatable Global Unicast—The aggregatable global unicast address uniquely identifies the client in global network and equivalent to public IPv4 address. A client can have multiple aggregatable global unicast addresses.

- **IP Type**—The IP address type can be IPv4 and IPv6.
  - Global Unique
  - Unique Local
  - Link Local

- **User Name**—Username based on 802.1x authentication. Unknown is displayed for client connected without a username.
- **Type**—Indicates the client type.
  - \( \text{\ding{60}} \) indicates a lightweight client
  - \( \text{\ding{61}} \) indicates a wired client
  - \( \text{\ding{62}} \) indicates an autonomous client
Vendor—Device vendor derived from OUI.

Device Name—Network authentication device name. For example, WLC and switch.

Location—Map location of the connected device.

VLAN—Indicates the access VLAN ID for this client.

Status—Current client status.
- Idle—Normal operation; no rejection of client association requests.
- Auth Pending—Completing a AAA transaction.
- Authenticated—802.11 authenticated complete.
- Associated—802.11 association complete. This is also used by wired clients to represent that a client is currently connected to the network.
- Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.
- To Be Deleted—The client is deleted after disassociation.
- Excluded—Automatically disabled by the system due to perceived security threat.

Interface—Controller interface (wireless) or switch interface (wired) that the client is connected to.

Protocol
- 80.2.11—wireless
- 802.3—wired

Association Time—Last association start time (for wireless client). For a wired client, this is the time when a client is connected to a switch port. This is blank for a client which is associated but has problems being on the network.

CCX—Lightweight wireless only.

Step 3 Select the radio button next to MAC Address in the Clients and Users page to view the associated client information. The following different client parameters appear.

- Client Attributes
- Client IPv6 Addresses
- Client Statistics

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

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

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

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

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

• Session—Lists the following client session information:
  -- Controller Name
  -- AP Name
  -- AP IP Address
  -- AP Type
  -- AP Base Radio MAC
  -- Anchor Address
  -- 802.11 State
  -- Association ID
  -- Port
  -- Interface
  -- SSID
  -- Profile Name
  -- Protocol
  -- VLAN ID
  -- AP Mode

• Security (wireless and Identity wired clients only)—Lists the following security information:
  -- Security Policy Type
- EAP Type
- On Network
- 802.11 Authentication
- Encryption Cipher
- SNMP NAC State
- RADIUS NAC State
- AAA Override ACL Name
- AAA Override ACL Applied Status
- Redirect URL
- ACL Name
- ACL Applied Status
- FlexConnect Local Authentication
- Policy Manager State
- Authentication ISE
- Authorization Profile Name
- Posture Status
- TrustSec Security Group
- Windows AD Domain

**Note**
The identity clients are the clients whose authentication type is 802.1x, MAC Auth Bypass or Web Auth. For non-identity clients, the authentication type is N/A.

**Note**
The data that appears under the client attributes differs based on identity and non-identity clients. For identity clients, you can see the security information such as Authentication status, Audit Session ID, and so on.

- Statistics (wireless only)
- Traffic—Shows the client traffic information.
- For wireless clients, client traffic information comes from controller. For wired clients, the client traffic information comes from ISE, and you must enable accounting information and other necessary functions on switches.

**Statistics**
The Statistics group box contains the following information for the selected client:
- Client AP Association History
- Client RSSI History (dBm)—History of RSSI (Received Signal Strength Indicator) as detected by the access point with which the client is associated.
- Client SNR History—History of SNR (signal-to-noise Ratio of the client RF session) as detected by the access point with which the client is associated.
- Bytes Sent and Received (Kbps)—Bytes sent and received with the associated access point.
• Packets Sent and Received (per sec)—Packets sent and received with the associated access point.
• Client Data rate

**Note** Hover your mouse cursor over points on the graph for additional statistical information.

**Client IPv6 Addresses**
The IPv6 address group box contains the following information for the selected client:

• IP Address—Shows the clients IPv6 address.
• Scope—Contains 3 types scope. They are Global Unique, Local Unique, and Link Local.
• Address Type—Shows the address type.
• Discovery Time—Time when the IP was discovered.

**Association History**
The association history dashlet shows information regarding the last ten association times for the selected client. This information helps in troubleshooting the client.

The Association History dashlet contains the following information:

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

**Events**
The Event group box of the Client Details page display all events for this client including the event type as well as the date and time of the event:

• Event Type
• Event Time
• Description

**Map**
Click View Location History to view location history details of wired and wireless clients.

You can view the location details for wired and wireless clients.

The following location history information is displayed for a wired or wireless client:

• Timestamp
• State
• Port Type
• Slot
• Module
Upgrading from 5.0 to 6.0 or 7.0

Caution
The number of supported clients, tags, and access points (wIPS) is reset to 100 clients, 100 tags, and 20 access points when you upgrade to Release 6.0 or later. All tracking beyond these limits is lost. These limits correspond to the 120-day evaluation licenses that are standard.

Caution
When upgrading the mobility services engine from 6.0 to 7.0, if any limits have been set on wireless clients or rogues, they are reset because of the wired client limit change in 7.0.

Caution
You must back up the mobility services engine database before upgrading from Release 5.1 or 6.0 to 7.0 to preserve client, tag, and access point configurations. You can restore the database after the software upgrade.

Note
Release 5.1 did not support licenses. You must order, register, and install licenses to track client and tag locations (CA) or access points (wIPS) beyond the limits of the 120-day evaluation licenses.

To upgrade to Release 7.0, follow these steps:

Step 1
Register the Product Authorization Key (PAK).

Note
You receive a PAK when you order a license. If you have lost your PAK, you can use your sales order or the UDI number of the mobility services engine to register.

• Client and wIPS licenses are registered at:
  www.cisco.com/go/license
• Tag licenses are registered at aeroscout website.

Step 2
Back up the mobility services engine database:
  a. Choose Services > Mobility Services.
  b. Click the name of the mobility services engine on which you want to back up.
  c. Choose System > Maintenance.
  d. Click Backup.
e. Enter the name of the backup file.

f. Click **Submit** to backup the historical data to the hard drive of the server running the Prime Infrastructure.

**Step 3** Download Release 7.0:

a. Choose **Services > Mobility Services**.

b. Click the name of the mobility services engine to which you want to download the software.

c. Choose **System > Maintenance > Download Software** from the left sidebar menu.

d. To download software, do one of the following:
   - To download software listed in the Prime Infrastructure directory, select the **Select from uploaded images to transfer** into the Server radio button. Choose a binary image from the drop-down list.
     
     The Prime Infrastructure downloads the binary image to the FTP server directory you specified during the Prime Infrastructure installation.
   
   - To use downloaded software available locally or over the network, select the **Browse a new software image to transfer into the Server** radio button and click **Choose File**. Locate the file and click **Open**.

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

**Step 4** Install Release 7.0 using the MSE CLI:

a. To overwrite existing software, enter:

```
/etc/init.d/msed stop
cd opt/installers
./<mse software file name>
```

b. To perform a fresh install, enter:

```
/etc/init.d/msed stop
cd /opt/mes/uninstall
./uninstall (enter this once in directory)
```

(Enter no when prompted to keep old database)

```
cd /opt/installers
./<mse software file name>
```

**Step 5** Restore the mobility services engine database (For Step 4 b.):

a. Choose **Services > Mobility Services**.

b. Click the name of the mobility services engine on which you upgraded the software.

c. Choose **Maintenance > Restore** from left sidebar menu.

d. Choose the filename to restore from the drop-down list. Click **Submit**.

**Step 6** Install the licenses.

Viewing the MSE Alarm Details

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

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

Table 16-15 describes the various fields in the Alarm Detail page for an MSE.

### Table 16-15  General Parameters

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

**Note**

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

- Related Alarm List—Displays all the alarms related to a particular attack.
- Rogue Client Details—Displays information about the rogue clients.
- Annotations—Enter any new notes in this text box and click **Add** to update the alarm. Notes appear in the “Annotations” display page.
- Messages—Displays information about the alarm.
- Device Details—
- Switch Port Tracing
- Location Notification
- Map Location
- Device Events
- Related History
• Audit Report—Click to view config audit alarm details. This report is only available for Config Audit alarms.

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

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

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

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

**Select a command**

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

• Assign to me—Assign the selected alarm(s) to the current user.
• Unassign—Unassign the selected alarm(s).
• Delete—Delete the selected alarm(s).
• Clear—Clear the selected alarm(s). Indicates that the alarm is no longer detected by any access point.

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

• Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the Prime Infrastructure and you can search for all Acknowledged alarms using the alarm search functionality.
• Unacknowledge—You can choose to unacknowledge an already acknowledged alarm.
• Email Notification—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications.
• Event History—Takes you to the Monitor > Events page to view events for this alarm.

**MSE License Overview**

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

• Context-Aware Service
• Wireless Intrusion Prevention System (wIPS)
• Location Analytics Service
• Mobile Concierge Service
• Mobile Billboard service

To enable smooth management of MSE and its services, various licenses are offered.
Note
You must have a Cisco Prime Infrastructure license to use MSE and its associated services.

MSE License Structure Matrix

Table 16-16 lists the breakdown of the licenses between the High-end, Low-end and Evaluation licenses for MSE, Location services, SCM, wIPS and MIR.

<table>
<thead>
<tr>
<th>MSE License Structure Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High End</strong></td>
</tr>
<tr>
<td><strong>MSE Platform</strong></td>
</tr>
<tr>
<td><strong>Context Aware Service</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>wIPS</strong></td>
</tr>
</tbody>
</table>

Sample an MSE License File

The following is a sample MSE license file:

```
FEATURE MSE cisco 1.0 permanent uncounted

VENDOR_STRING=UDI=udi,COUNT=1

HOST ID=ANY

NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</LicLineID> <PAK>dummyPak</PAK>"

SIGN="0C04 1EBA BE34 F208 404F 98ED 43EC 45D7 F881 08F6 7PA5 4DED 43BC AF5C C359 0444 36B2 45CF 6EA6 1DB1 899F 413F F543 F426 B055 4C7A D95D 2139 191F 04DE"
```

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

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

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

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

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

Deploying the MSE Virtual Appliance

MSE is also offered as a virtual appliance. The MSE virtual appliance software is distributed as an Open Virtualization Archive (OVA) file.

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

**Note**  
See the Cisco Prime Infrastructure Getting Started Guide, Release 1.0 for more information on the physical appliance.

When the MSE is located on the physical appliance, the license installation process is based on Cisco UDI (Unique Device Identifier). Choose Administration > License Center on the Prime Infrastructure UI to add the license. When the MSE is located on the virtual appliance, the license installation is done using a VUDI (Virtual Unique Device Identifier) instead of UDI.

**Note**  
MSE is available as a virtual appliance for this release and later. Virtual appliance must be activated first before installing any other service licenses.

For a virtual appliance, you must have an activation license. Without an activation license, if the MSE starts in evaluation mode even if the licenses are present on the host, it rejects the permanent license if the activation license is not installed. If the virtual appliance is added to the Prime Infrastructure, the Prime Infrastructure does not allow the MSE to be synchronized unless the activation license is added to the MSE.

**Note**  
Virtual licenses are not allowed on physical appliances.

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

See the “Adding a License File to the MSE Using the License Center” section on page 16-814 and the “Deleting an MSE License File” section on page 16-726 for more information on adding a license and deleting a license using the Mobility Services Engine wizard.
Adding a License File to the MSE Using the License Center

To add a license, follow these steps:

Step 1. Install the MSE virtual appliance.
Step 2. Add the MSE to the Prime Infrastructure using the “Adding a Mobility Services Engine” section on page 16-723.
Step 3. Choose Administration > License Center on the Prime Infrastructure UI to access the License Center page.
Step 4. Choose Files > MSE Files from the left sidebar menu.
Step 5. Click Add to add a license.
Step 6. Select the MSE and browse to the activation license file.
Step 7. Click Submit.

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

Viewing the MSE License Information using License Center

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

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

The MSE Summary page displays the following information. See Table 16-17.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSE Name</td>
<td>Provides a link to the MSE license file list page.</td>
</tr>
<tr>
<td>Service</td>
<td>Type of service using: CAS or wIPS.</td>
</tr>
<tr>
<td>Platform Limit by AP</td>
<td>Platform limit.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type of MSE.</td>
</tr>
<tr>
<td>Installed Limit by AP</td>
<td>Displays the total number of client elements licensed across MSEs.</td>
</tr>
<tr>
<td>License Type</td>
<td>The three different types of licenses. They are permanent, evaluation, and extension.</td>
</tr>
<tr>
<td>Count by elements</td>
<td>The number of CAS or wIPS elements currently licensed across MSEs.</td>
</tr>
<tr>
<td>Unlicensed Count</td>
<td>Displays the number of client elements that are not licensed.</td>
</tr>
<tr>
<td>%Used</td>
<td>The percentage of CAS or wIPS elements licensed across MSEs.</td>
</tr>
</tbody>
</table>
Removing a License File Using the License Center

To remove a license, follow these steps:

1. **Step 1** Install the MSE virtual appliance.
2. **Step 2** Add MSE to Prime Infrastructure using the wizard.
3. **Step 3** Choose Administration > License Center on the Prime Infrastructure UI to access the License Center page.
4. **Step 4** Choose Files > MSE Files from the left sidebar menu.
5. **Step 5** Choose an MSE license file that you want to remove by selecting the radio button, and click Remove.
6. **Step 6** Click OK to confirm the deletion.

Auto Switch Port Tracing and Auto Containment of Rogue APs

Currently, the Prime Infrastructure provides rogue access point detection by retrieving information from the controller. The rogue access point table is populated with any detected BSSID addresses from any frames that are not present in the neighbor list. At the end of a specified interval, the contents of the rogue table are sent to the controller in a CAPWAP Rogue AP Report message. With this method, the Prime Infrastructure simply gathers the information received from controllers; but from the software Release 5.1, you can incorporate switch port tracing of wired rogue access point switch ports.

The auto SPT and containment is introduced in Release 7.3. The auto SPT is more preferable for a large wireless network. The auto SPT starts automatically when a rogue AP is reported to the Prime Infrastructure. The auto SPT complements to manual SPT feature by providing a quicker scan based on the wired location association of the rogue AP. The Prime Infrastructure UI allows you to configure the criteria for auto SPT and auto containment so that you can run a trace and contain the detected rogue access points on the wire.

When the multiple controllers report that a rogue AP should be auto contained, the Prime Infrastructure finds the controller that reports the strongest RSSI sends the containment request to the controller.

Configuring Auto Switch Port Tracing Criteria on the Prime Infrastructure

To configure auto switch port tracing settings on the Prime Infrastructure, follow these steps:

1. **Step 1** Choose Administration > System Settings.
2. **Step 2** From the left sidebar menu, choose Rogue AP Settings. The Rogue AP Settings page appears.
3. **Step 3** Select the Enable Auto Switch Port Tracing check box to allow the Prime Infrastructure to automatically trace the switch port to which the rogue access point is connected. You can configure the following parameters:
   - Repeat Search After—Enter the number of minutes after which you want the Prime Infrastructure to automatically repeat the search for Rogue APs. By default, the Prime Infrastructure repeats the search for Rogue APs every 120 minutes.
• Allow Trace For Found On Wire Rogue AP—Select the check box to enable auto SPT to trace wired rogue APs.
• Critical—Select the check box to set the alarm severity to critical.
• Major—Select the check box to set the alarm severity to major.
• Minor—Select the check box to set the alarm severity to minor.

Step 4
Click Ok.

Configuring Auto Containing Settings on the Prime Infrastructure

To configure auto containment settings on the Prime Infrastructure, follow these steps:

Step 1
Choose Administration > Settings.

Step 2
From the left sidebar menu, choose Rogue AP Settings. The Rogue AP Settings page appears.

Step 3
Select the Enable Auto Containment check box to allow the Prime Infrastructure to trigger auto containment when a rogue AP is received by the Prime Infrastructure. You can configure the following parameters:

• Exclude Rogue APs Found On Wire By Switch Port Tracing—Select the check box to automatically exclude those APs that are detected on the wired network through auto SPT.
• Critical—Select the check box to set the alarm severity to critical.
• Major—Select the check box to set the alarm severity to major.
• Containment Level—Select the check box enable the auto containment level. This indicates the containment level of the rogue APs.
  – 1 AP Containment—Target the rogue access point for containment by one access point. (Lowest containment level). When you select this, one access point in the vicinity of the rogue unit sends deauthenticate and disassociate messages to the client devices that are associated to the rogue unit.
  – 2 AP Containment—Target the rogue access point for containment by two Cisco lightweight access points. Two access points in the vicinity of the rogue unit send deauthenticate and disassociate messages to the rogues clients
  – 3AP Containment—Target the rogue access point for containment by three Cisco lightweight access points.
  – 4AP Containment—Target the rogue access point for containment by four Cisco lightweight access points. (Highest containment level).

Note
The higher the threat of the rogue access point, the higher the containment required.

Caution
Attempting to contain a rogue access point might lead to legal consequences. When you select any of the AP Containment commands and click Go, a message “Containing a Rogue AP may have legal consequences. Do you want to continue?” appears. Click OK if you are sure or click Cancel if you do not wish to contain any access points.
Step 4  Click OK.

Location Assisted Client Troubleshooting from the Context Aware Dashboard

You can use the Context Aware dashboard on the Prime Infrastructure home page to troubleshoot a client. You can specify a MAC address or Username or IP address as the search criteria, and click Troubleshoot.

Note: Username, IP address, and partial MAC address-based troubleshooting is supported only on MSEs Version 7.0.200.0 and later.

The Troubleshoot Client page appears.
You can view the Context Aware History report on the Context Aware History tab.
You can filter this report based on MSE Name. You can further filter the report based on Timezone, State or All. The states can be either associated or dissociated.
If you select timezone, then you can choose any of the following:
  • Date and Time
  Or
  • Any one of these values from the drop-down list:
    – Last 1 Hour
    – Last 6 Hours
    – Last 1 Day
    – Last 2 Days
    – Last 3 Days
    – Last 4 Days
    – Last 5 Days
    – Last 6 Days
    – Last 7 Days
    – Last 2 Weeks
    – Last 4 Weeks
Alternately, you can use the Generate Report link to generate a Client Location History report. You can also opt to export to CSV or PDF format or e-mail the report using the icons available in the report page.

**MSE Analytics Reports**

You can generate many MSE Analytics reports using the Report Launch Pad.

**Monitoring Maps**

Maps provide a summary view of all your managed system on campuses, buildings, outdoor areas, and floors. See the “About Maps” section on page 6-153 for more information on maps.

**Mobile Concierge Service**

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

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, mae product suggestions, allow you to organize shopping lists, receive unique digital signature based on shopping preferences.

**Related Topics**

- Licensing for Mobile Concierge
- Defining a Venue
- Deleting the Venue
- Defining a Provider with Policies
- Deleting the Provider
- Defining New Policies
- Deleting New Policies

**Licensing for Mobile Concierge**

The Mobile Concierge service can be enabled only if you have a valid advanced location license (Base location license, Mobile Concierge, and Analytics license). The evaluation license is valid for 120 days and the permanent license is based on the MSE platform and the number of service advertisements supported.
Defining a Venue

To define a venue, follow these steps:

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

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

The 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.

### Deleting the Venue

To delete a venue, follow these steps:

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

The Venues page appears.

**Step 2** Select the check box of the venue that you want to delete.

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

**Step 4** Click **OK** to confirm the deletion.

### Defining a Provider with Policies

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

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

The Providers page appears.

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

The Provider Wizard page appears.

**Step 4** Enter the 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 blue inverted triangle icon location at the left side of the Local Service # name to expand the Local Service and configure the following:
  - Choose the service type from the Service Type drop-down list. The possible options are: Directory Info, Sign Up, Discount Coupon, Network Help, and Other.
  - Enter the display name in the Display Name text box.
  - Enter the description in the Description text box.
  - Choose the service URIs from the drop-down list.
  - Recommended Apps - recommended application for the venue.
Chapter 16    Prime Infrastructure Services

Mobile Concierge Service

Step 9   Click Save.

Deleting the Provider

To delete a venue, follow these steps:

---

Step 1   Choose Services > Mobile Concierge.

The Venues page appears.

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

The Providers page appears.

Step 3   Select the check box of the provider that you want to delete.

Step 4   From the Select a command drop-down list, choose Delete Provider, and click Go.

Click OK to confirm the deletion.

---

Defining New Policies

To define policies, follow these steps:

---

Step 1   Choose Services > Mobile Concierge.

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

The Policies page appears.

Step 3   From the Select a command drop-down list, choose Define New Policy and click Go.

The Policy Wizard page appears.

Step 4   Choose the venue on which you want the policy to be applied from the Venue drop-down list.

Step 5   Click Next. The Provider group box appears.

Step 6   Choose the provider from the Provider drop-down list.

Step 7   Click Next. The SSID group box appears.

Step 8   From the SSID drop-down list, choose the SSIDs on which you want to broadcast the service advertisements and click OK. You can choose multiple SSIDs.

Step 9   Click Next. The Display Rule group box appears.

Step 10  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.
Deleting New Policies

To delete a venue, follow these steps:

Step 1 Choose Services > Mobile Concierge.
The Venues page appears.

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

Step 3 Select the check box of the policy that you want to delete.

Step 4 From the Select a command drop-down list, choose Delete Policy, and click Go.
Click OK to confirm the deletion.

Adding Service Advertisements to the Floor Map

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

Step 1 Choose Monitor > Site Maps.
The Site Maps page appears.

Step 2 Choose the appropriate floor location link from the list.
A map appears showing the placement of all installed access points, client, and tags and their relative signal strength.

Step 3 Click the Services icon on the floor map page.
The Venue dialog box to associate service advertisement to that particular venue appears.

Step 4 Click the Show/Associate Services link to open the Add/Edit Mobile Concierge Service Services page.
The list of all the available service advertisements are displayed and you can associate service advertisements by selecting them.

Step 5 To associate a service advertisement, you can do the following:

- Choose an advertisement by filtering based on either the provider name or friendly name by choosing them from the Filter By drop-down list.

  or

- Select the Associate check box to associate that particular service advertisement.
Creating Service Advertisements from the Floor Map

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

Step 1 Choose Monitor > Site Maps.
The Site Maps page appears.

Step 2 Choose the appropriate floor location link from the list.
A map appears showing the placement of all installed access points, client and tags, and their relative signal strength.

Step 3 Click the Services icon on the floor map page.
The Venue dialog box to associate service advertisement to that particular venue appears.

Step 4 Click the Show/Associate Services link to open the Add/Edit Mobile Concierge Services.
The list of all the available service advertisements is displayed and you can associate service advertisements by choosing them.

Step 5 Click Create Mobile Concierge Service to create service advertisements.
You are redirected to the Service > Mobile Concierge > Add Service Advertisements page.

Step 6 Follow the steps in the “Adding Service Advertisements to the Floor Map” section on page 16-822 to create the service advertisements provided.

Related Topics

- Adding Service Advertisements to the Floor Map
- Viewing the Configured Service Advertisements
- Viewing Mobile Concierge Service Statistics
- Viewing the MSE Summary Page for Mobile Concierge License Information
- Viewing Service Advertisements Synchronization Status
- Adding a Mobile Concierge Service License Using the License Center
- Mobile Concierge Reports

Viewing the Configured Service Advertisements

To view the configured service advertisements, follow these steps:

Step 1 Choose Services > Mobility Services Engine.

Step 2 Click Device Name to view its properties.
The General Properties page appears.
**Step 3** Choose **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.

---

**Related Topics**

- Adding Service Advertisements to the Floor Map
- Viewing Mobile Concierge Service Statistics
- Viewing the MSE Summary Page for Mobile Concierge License Information
- Viewing Service Advertisements Synchronization Status
- Adding a Mobile Concierge Service License Using the License Center
- Mobile Concierge Reports

---

**Viewing Mobile Concierge Service Statistics**

To view Mobile Concierge Service statistics, follow these steps:

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

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

The General Properties page appears.

**Step 3** Choose **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.

---

**Related Topics**

- Adding Service Advertisements to the Floor Map
- Viewing the Configured Service Advertisements
- Viewing the MSE Summary Page for Mobile Concierge License Information
- Viewing Service Advertisements Synchronization Status
- Adding a Mobile Concierge Service License Using the License Center
Mobile Concierge Reports

Viewing the MSE Summary Page for Mobile Concierge License Information

See the “Performing Administrative Tasks” section on page 15-717 for more information on MSE licensing.

Viewing Service Advertisements Synchronization Status

To view service advertisements synchronization status, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Services &gt; Synchronize Services.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose Service Advertisements from the left side menu bar.</td>
</tr>
</tbody>
</table>

The following information appears in the Service Advertisements page:

- Provider Name—Shows the name of the service provider.
- Service—Shows the type of service that a particular advertisement is using.
- MSE—Shows whether the service advertisement is synchronized with the MSE or not.
- Sync Status—Shows the synchronization status. A green two-arrow icon indicates that its corresponding element is synchronized with the given server such as MSE. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a given server.
- Message—Shows any message related to the advertisement synchronization failure.

Related Topics

- Adding Service Advertisements to the Floor Map
- Viewing Mobile Concierge Service Statistics
- Viewing the MSE Summary Page for Mobile Concierge License Information
- Adding a Mobile Concierge Service License Using the License Center
- Mobile Concierge Reports

Adding a Mobile Concierge Service License Using the License Center

To add a Mobile Concierge service license using the license center, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; Licenses.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose Files &gt; MSE Files from the left sidebar menu. The License Center page appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Add to select the license file.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click OK to add the license.</td>
</tr>
</tbody>
</table>
The Mobile Concierge Service license is added.

Related Topics

- Adding Service Advertisements to the Floor Map
- Viewing Mobile Concierge Service Statistics
- Viewing the MSE Summary Page for Mobile Concierge License Information
- Viewing Service Advertisements Synchronization Status
- Mobile Concierge Reports

Mobile Concierge Reports

You can generate 2 types of Mobile Concierge reports:

- Service URI Statistics—In this report, you can retrieve information about the top services that you have used based on the filters like venue, provider, mobile mac. With this report, you can get the additional information about the usage of the services across a given venue.
- Mobile MAC Statistics—In this report, you can retrieve information about the most active clients based on the filters like venue. With this report, you can get additional information about the most active mobiles in a given venue.

Identity Services

Cisco Identity Services Engine (ISE) is a next-generation identity and policy-based network access platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations.

The Prime Infrastructure manages the wired and the wireless clients in the network. When Cisco ISE is used as a RADIUS server to authenticate clients, the Prime Infrastructure collects additional information about these clients from the ISE and provides all relevant client information to the Prime Infrastructure to be visible in a single console.

Note

The Prime Infrastructure communicates with the ISE using REST API. See http://www.cisco.com/en/US/docs/security/ise/1.0/api_ref_guide/ise10_api_ref_guide_ch1.html for more information on Cisco ISE APIs.

Note

Accounting data for wired clients are collected from ISE every 15 minutes. There is a background ISE Status task that polls all ISEs added to the Prime Infrastructure for every 15 minutes for the status of ISEs and updates the status.

The ISE integration in the Prime Infrastructure provides the following features:

- Periodic polling to the ISE for collecting client statistics and other attributes requires for client list, dashboard charts, and reports.
• On demand query to the ISE for getting additional client details such as Authorization Profile, Posture, Endpoint Type (profiler), and so on.
• Cross launch the ISE user interface with automatic single sign on.

See the Cisco Identity Services Engine User Guide, Release 1.0 at the following URL: http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html for more information about ISE.

This section contains the following topics:
• Viewing Identify Services, page 16-827
• Adding an Identity Services Engine, page 16-827
• Removing an Identity Services Engine, page 16-828

Viewing Identify Services

To see the Identity Services Engines that are added in the Prime Infrastructure, choose Services > Identity Services. The following parameters appear:
• Server Address—IP address of ISE.
• Port—HTTPS port number for the server.
• Retries—Indicates the number of retry attempts.
• Version—Indicates the version of the ISE.
• Status—Indicates the reachability status, that is, Reachable or Unreachable.
• Role—Indicates if a node is a primary, standalone or, standby node.

Adding an Identity Services Engine

Note A maximum of two ISEs can be added in the Prime Infrastructure. If you add two ISEs, one should be primary and the other should be standby. When you are adding a standalone node, you can add only one standalone node and cannot add second node.

To add an Identity Services Engine, follow these steps:

Step 1 Choose Services > Identity Services.

Step 2 From the Select a command drop-down list, choose Add Identity Services Engine.

Step 3 In the Server Address text box, type the IP address of the server.

Step 4 In the Port text box, enter the port number of the server. The default is 443.

Step 5 In the Username text box, enter the username.

Step 6 In the Password text box, enter the password.

Step 7 Reenter the password in the Confirm Password text box.

Note The credentials should be superuser credentials. Otherwise, ISE integration does not work.
Removing an Identity Services Engine

To remove an Identity Services Engine, follow these steps:

**Step 1** Choose Services > Identity Services.

**Step 2** Select the check box(es) of the identity services engines that you want to delete.

**Step 3** From the Select a command drop-down list, choose Delete Identity Services Engine(s).

**Step 4** Click OK to confirm the deletion.

---

**Step 8** In the HTTP Connection Timeout text box, enter the amount of time (in seconds) allowed before the process time out. The default is 30 seconds.

**Step 9** Click Save.