Configuring MSE System Settings and Services

- Viewing Dashboard, page 2
- Viewing and Adding License, page 2
- Adding Users, page 3
- Deleting Users, page 4
- Changing User Properties, page 4
- Adding User Groups, page 4
- Deleting User Groups, page 5
- Changing User Group Permissions, page 5
- Viewing Server Events, page 6
- Viewing Audit Logs, page 6
- Viewing NMSP Status, page 7
- Verifying an NMSP Connection to a Mobility Services Engine, page 8
- Backing Up Mobility Services Engine Historical Data, page 8
- Restoring Mobility Services Engine Historical Data, page 9
- Downloading Software to the Mobility Services Engines, page 9
- Configuring Tracking Parameters for a Mobility Services Engine, page 10
- Configuring Filtering Parameters for a Mobility Services Engine, page 12
- Configuring Mobility Services Engine History Parameters, page 13
- Enabling and Configuring Location Presence on a Mobility Services Engine, page 14
- Exporting Asset Information, page 15
- Importing Asset Information, page 16
- Configuring Location Parameters, page 16
- Configuring Notification Parameters, page 20
- Viewing Notification Statistics, page 21

- Configuring Qualcomm PDS, page 23
- Enabling Mobile Applications, page 23

Viewing Dashboard

To view the dashboard, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **System > Dashboard**.
You will be able to view the following details in the dashboard:

- No of active clients
- Percentage of memory utilization
- Percentage of CPU utilization
- Notification Destinations
- MAC Filtering Status - Enabled or Disabled
- Client Location History - Enabled or Disabled
- Location calculation latency
- Type of license used
- Number of controllers synched

Viewing and Adding License

To view and add license to the MSE, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

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

Step 4 The License page displays the following information.

Field	Description
Type	Type of service.
Platform Limit	Platform Limit

Field	Description
Installed Limit	Displays the total number of client elements licensed across MSEs.
License Type	The three different types of licenses. They are permanent, evaluation, and extension.

Step 5 Click **Select File** to browse for the license file.

Step 6 Click **Add** to add the license to the MSE.

Adding Users

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

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

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

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

Step 4 Click **Add User**.

Step 5 Enter the username in the Username text box.

Step 6 Enter a password in the Password text box.

Step 7 Re-enter the password in the Confirm Password text box.

Step 8 Enter the name of the group to which the user belongs in the Group Name text box.

Step 9 From the Permission drop-down list, choose a permission level (**read**, **write**, or **full**).

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

Step 10 Click **Save**.

Deleting Users

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

Step 1 Launch the MSE admin UI.
Step 2 Click the Configuration icon on the top right of the home page.
Step 3 Choose **System** > **Accounts** > **Users**.
Step 4 Click the **Delete** icon corresponding to the user details that you want you delete.
Step 5 Click **OK**.

Changing User Properties

To change user properties, follow these steps:

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

Adding User Groups

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

Step 1 Launch the MSE admin UI.
Step 2 Click the Configuration icon on the top right of the home page.
Step 3 Choose **System** > **Accounts** > **Groups**.
Step 4 Click **Add Group**.
Step 5 Enter the name of the group in the **Group Name** text box.
Step 6 Choose a permission level (**read**, **write**, or **full**) from the Permission drop-down list.
Note Full access is required for the Prime Infrastructure to access mobility services engines.

Step 7 Click **Save**.

Deleting User Groups

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

Step 1 Launch the MSE admin UI.
Step 2 Click the Configuration icon on the top right of the home page.
Step 3 Choose **System** > **Accounts** > **Groups**.
Step 4 Click the **Delete** icon corresponding to the user group that you want to delete.
Step 5 Click **OK**.

Changing User Group Permissions

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

To change user group permissions, follow these steps:

Step 1 Launch the MSE admin UI.
Step 2 Click the Configuration icon on the top right of the home page.
Step 3 Choose **System** > **Accounts** > **Groups**.
Step 4 Click the name of the group you want to edit.
Step 5 From the Permission drop-down list, choose a permission level (**read**, **write**, **full**).
Step 6 Click **Save.**

Viewing Server Events

To view server events, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **System > Status > Server Events**.
The Server Events page appears.

The following table lists the server events page fields.

Field	Description
Timestamp	Timestamp when the event occurred.
Severity	Severity of the event.
Event	A description of the event.
Facility	Facility parameter.

Viewing Audit Logs

To view audit logs, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **System > Status > Audit Logs**.
The Audit Logs page appears.

The following table lists the audit logs page fields.

Field	Description
User Name	Admin user id.
Operation	Description of the operation performed.
Operation Status	Status of the operation.
Module	The name of the module that performed the operation.
Invocation Time	Time when the operation was invoked.

Viewing NMSP Status

To configure NMSP status, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

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

Step 4 The following table lists the NMSP parameters.

Table 1: NMSP Parameters

Field	Description
IP Address	
Target Type	
Version	
NMSP Status	
Echo Request Count	
Echo Response Count	
Last Message Received	

Step 5 Click on the IP address to get a detailed report on the NMSP status.

Verifying an NMSP Connection to a Mobility Services Engine

To verify an NMSP connection between a mobility services engine and a controller or a location-capable Catalyst switch, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **System** > **Status** > **NMSP Status**.

Step 4 Verify that the NMSP Status is ACTIVE.
If not active, resynchronize the Catalyst switch or controller and the mobility services engine.

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

Backing Up Mobility Services Engine Historical Data

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

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

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

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

Step 4 Enter the FTP server address.

Step 5 Enter the port number of the FTP server.

Step 6 Enter the timeout value in seconds.

Step 7 Enter the username of the backup server.

Step 8 Enter the password of the backup server.

Step 9 Enter the server filename.

Step 10 Click **Backup** to back up the historical data to the hard drive of the server running Prime Infrastructure.
The Status of the backup is visible on the page while the backup is in process. Three items appear in the page during the backup process: (1) Last Status text box that provides messages noting the status of the backup; (2) Progress text box that shows what percentage of the backup is complete; and (3) Started at text box that shows when the backup began noting date and time.

Note You can run the backup process in the background while working on other mobility services engine operations in other the Prime Infrastructure pages. Backups are stored in the FTP directory that you specify during the Prime Infrastructure installation.

Restoring Mobility Services Engine Historical Data

You can use the Prime Infrastructure to restore backed up historical data.

To restore mobility services engine data, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

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

Step 4 Enter the port number of the FTP server.

Step 5 Enter the timeout value in seconds.

Step 6 Enter the username.

Step 7 Enter the password.

Step 8 Click **Show Backup Files** to view the backup files.

Step 9 Click **Submit** to start the restoration process.

Step 10 Click **OK** to confirm that you want to restore the data from the Prime Infrastructure server hard drive. When restoration is completed, the Prime Infrastructure displays a message to that effect.

Note You should not work on other mobility services engine operations when the restore process is running.

Downloading Software to the Mobility Services Engines

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

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **System** > **Maintenance** > **Download Software** from the left sidebar menu.

Step 4 To downloaded software available locally or over the network, click **Select File**. Locate the file, and click **Open**.

Step 5 Click **Import** to send the software to the /opt/installers directory on the mobility services engine.

Step 6 After the image is transferred to the mobility services engine, log in to the mobility services engine command-line interface.

Step 7 Run the installer image from the /opt/installers directory by entering the **./.bin mse image** command. This installs the software.

Step 8 To run the software, enter the /etc/init.d/msed start command.

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

Configuring Tracking Parameters for a Mobility Services Engine

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

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **Context Aware Service** > **Tracking** to display the configuration options.

Step 4 Modify the tracking parameters as appropriate. The following table lists the tracking parameters.

Table 2: Tracking Parameters

Field	Configuration Options
Tracking Parameters	
Wired Clients	**1** Select the **Enable** check box to enable tracking of client stations by the mobility services engine. In Release 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers. The wired client limiting is supported from mobility services engine 7.0 and Prime Infrastructure Release 7.0 and later. In other words, you can limit wired clients to a fixed number such as 500. This limit is set to ensure that the licenses are not taken up completely by wired clients and some licenses are available for wireless clients. **Caution** When upgrading the mobility services engine from Release 6.0, if any limits have been set on wireless clients or rogues, they are reset because of the wired client limit change in Release 7.0. **Note** Active Value (display only): Indicates the number of wired client stations currently being tracked. **Note** Not Tracked (display only): Indicates the number of wired client stations beyond the limit.
Wireless Clients	**1** Select the **Enable** check box to enable tracking of client stations by the mobility services engine. **2** Select the **Enable Limiting** check box to set a limit on the number of client stations to track. **3** Enter a Limit Value if limiting is enabled. The limit entered can be any positive value up to 18,000 which is the maximum number of clients that can be tracked by a mobility services engine. **Note** Active Value (Display only): Indicates the number of client stations currently being tracked. **Note** Not Tracked (Display only): Indicates the number of client stations beyond the limit.

Field	Configuration Options
Rogue Access Points	**1** Select the **Enable** check box to enable tracking of rogue access points by the mobility services engine. **2** Select the **Enable Limiting** check box to set a limit on the number of rogue access points to track. **3** Enter a Limit Value if limiting is enabled. The limit entered can be any positive value up to18,000 which is the maximum number of rogue access points that can be tracked by a mobility services engine. **Note** Active Value (Display only): Indicates the number of rogue access points currently being tracked. **Note** Not Tracked (Display only): Indicates the number of rogue access points beyond the limit.
Exclude Ad-Hoc Rogues	Select the check box to turn off the tracking and reporting of ad hoc rogues in the network. As a result, ad hoc rogues are not displayed on Prime Infrastructure maps or its events and alarms reported.
Rogue Clients	**1** Select the **Enable** check box to enable tracking of rogue clients by the mobility services engine. **2** Select the **Enable Limiting** check box to set a limit on the number of rogue clients to track. **3** Enter a Limit Value if limiting is enabled. The limit entered can be any positive value. This limit varies based on the platform. The limit value is the maximum number of rogue clients that can be tracked by a mobility services engine. **Note** Active Value (Display only): Indicates the number of rogue clients being tracked. **Note** Not Tracked (Display only): Indicates the number of rogue clients beyond the limit.
Interferers	**1** Select the **Enable** check box to enable tracking of the interferers by the mobility services engine. **2** Select the **Enable Limiting** check box to set a limit on the number of interferers to track. **3** Enter a Limit Value if limiting is enabled. In Release 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers. In Release 7.0.200.x, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, interferers, and guests. **Note** Active Value (Display only): Indicates the number of interferers currently being tracked. **Note** Not Tracked (Display only): Indicates the number of interferers beyond the limit.

Field	Configuration Options
Active RFID Tags	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. **Note** Not Tracked (Display only): Indicates the number of active RFID tags beyond the limit.

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

Configuring Filtering Parameters for a Mobility Services Engine

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

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **Context Aware Service** > **Filtering** to display the configuration options.

Step 4 Modify the filtering parameters as appropriate. The following table lists filtering parameters.

Table 3: Filtering Parameters

Field	Configuration Options
Advanced Filtering Params	
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 CAS 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 chose to specify a filter for interferers based on the duty cycle of the interferer.
RSSI Cutoff for Probing Clients	Enter the RSSI cutoff value for probing clients so that those clients whose RSSI values are below a cutoff value is reported. The default value for the RSSI cutoff for probing clients 1 -128dB.
MAC Filtering Params	
Exclude Probing Clients	Select the check box to prevent calculating location for probing clients.

Field	Configuration Options
Enable Location MAC Filtering	1 Select the check box to enable filtering of specific elements by their MAC addresses. 2 To import a file of MAC addresses (Upload a file for Location MAC Filtering text box), browse for the file name and click **Save** to load the file. MAC addresses from the list auto-populate the Allowed List and Disallowed List based on their designation in the file. **Note** To view allowed MAC address formats, click the icon next to the Upload a file for Location MAC Filtering text box. 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 then press **Ctrl** and click additional MAC addresses. Click **Allow** or **Disallow** to place an address in that column. **Note** If a MAC address is not listed in the Allow or Disallow column, it appears in the Blocked MACs column by default. If you click the Unblock button, the MAC address automatically moves to the Allow column. You can move it to the Disallow column by clicking the Disallow button under the Allow column.

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

Configuring Mobility Services Engine History Parameters

To configure mobility services engine history, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **Context Aware Service** > **History**.

Step 4 Modify the following history parameters as appropriate. The following table lists history parameter.

Table 4: History Parameters

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

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

Enabling and Configuring Location Presence on a Mobility Services Engine

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

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **Context Aware Service** > **Presence**. The Presence page appears.

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

Step 5 Select one of the following Location Resolution options:

a) When Building is selected, the 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 6 Select any or all of the location formats check boxes:

a) Select the **Cisco** check box to provide location by campus, building, floor, and X and Y coordinates. This is the default setting.
b) Select the **Civic** check box to provide the name and address (street, city, state, postal code, country) of a campus, building, floor, or outdoor area.
c) Select the **GEO** check box to provide the longitude and latitude coordinates.

Step 7 By default, the Text check box for Location Response Encoding is selected. It indicates the format of the information when received by the client. There is no need to change this setting.

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

Step 9 Enter a Retention Expiration value in minutes. This determines how long the received information is stored by the client before it is overwritten. The default value is 24 hours (1440 minutes).

Step 10 Click **Save**.

Exporting Asset Information

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

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **Context Aware Service** > **Asset Information**.
Information in the exported file is in the following formats:

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

Step 4 Click **Export**.

Step 5 Click **Open** (display to page), **Save** (to external PC or server), or **Cancel**.

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

Importing Asset Information

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

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

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

Step 4 Enter the name of the text file or browse for the filename.
Specify information in the imported file in the following formats:

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

Step 5 Click **Import**.

Configuring Location Parameters

To configure location parameters, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **Context Aware Service** > **Advanced Configuration**. The configuration options appear.

Step 4 Modify the location parameters as appropriate. The following table lists location parameters.

Table 5: Location Parameters

Field	Configuration Options
Enable Calculation time	Select the **Enable** check box to initiate the calculation of the time required to compute location. **Note** This parameter applies only to clients, rogue access points, rogue clients, and interferers. **Caution** Enable this parameter only under Cisco TAC personnel guidance because it slows down the overall location calculations.
Enabled OW Location	Select the **Enable** check box to include Outer Wall (OW) calculation as part of location calculation. **Note** This parameter is ignored by the mobility services engine.
Enable Data Accuracy Tool	Select the **Enable** check box to enable the Data Accuracy Tool. This parameter is disabled by default. **Note** The Data Accuracy Tool is a web application that displays in the MSE admin UI. Use this tool to filter the devices outside the venue using location tuning, maximum RSSI threshold, and based on stationary devices and MAC addresses. To use the Data Accuracy tool, enable the **Beta Features** from the MSE admin UI. After the beta features are enabled, scroll down to the bottom of the MSE admin UI and run the tool. For more information about the Data Accuracy Tool, see Using Data Accuracy Tool.
Relative discard RSSI time	Enter the number of minutes since the most recent RSSI sample after which RSSI measurement should be considered discarded. For example, if you set this parameter to 3 minutes and the mobility services engine receives two samples at 10 and 12 minutes, it keeps both samples. An additional sample received at 15 minutes is discarded. The default value is 3. Allowed values range from 0 to 99999. A value of less than 3 is not recommended. **Note** This parameter applies only to clients, rogue access points, rogue clients, and interferers.
Absolute discard RSSI time	Enter the number of minutes after which RSSI measurement should be considered stale and discarded, regardless of the most recent sample. The default value is 60. Allowed values range from 0 to 99999. A value of less than 60 is not recommended. **Note** This parameter applies only to clients.

Field	Configuration Options
RSSI Cutoff	Enter the RSSI cutoff value, in decibels (dBs) with respect to one (1) mW (dBm), above which the mobility services engine will always use the access point measurement. The default value is –75. **Note** When 3 or more measurements are available above the RSSI cutoff value, the mobility services engine discards any weaker values (lower than the RSSI cutoff value) and uses the 3 (or more) strongest measurements for calculation; however, when only weak measurements below the RSSI cutoff value are available, those values are used for calculation. **Note** This parameter applies only to clients. **Caution** Modify only under Cisco TAC personnel guidance. Modifying this value can reduce the accuracy of location calculation.
Enable Location Filtering	Location filtering is used to smooth out the jitters in the calculated location. This prevents the located device from jumping between two discrete points on the floor map.
Chokepoint Usage	Select the **Enable** check box to enable chokepoints to track Cisco-compatible tags.
Use Chokepoints for Interfloor conflicts	Perimeter chokepoints or weighted location readings can be used to locate Cisco-compatible tags. Options: • Never: When selected, perimeter chokepoints are not used to locate Cisco-compatible tags. • Always: When selected, perimeter points are used to locate Cisco-compatible tags. • Floor Ambiguity: When selected, both weighted location readings and perimeter chokepoints are used to locate Cisco-compatible tags. If similar locations are calculated by the two methods, the perimeter chokepoint value is used by default.
Chokepoint Out of Range timeout	When a Cisco-compatible tag leaves a chokepoint range, the timeout period entered is the period that passes before RSSI values are again used for determining location.
Absent Data cleanup interval	Enter the number of minutes that data for *absent* mobile stations is kept. An *absent* mobile station is one that was discovered but does not appear in the network. The default value is 1440.
Use Default Heatmaps for Non Cisco Antennas	Select this check box to enable the usage of default heatmaps for non-Cisco antennas during the Location Calculation. This option is disabled by default.
Movement Detection Parameters	

Field	Configuration Options
Individual RSSI change threshold	This parameter specifies the Individual RSSI movement recalculation trigger threshold. Enter a threshold value between 0-127 dBm. Modify only under Cisco TAC personnel guidance.
Aggregated RSSI change threshold	This parameter specifies the Aggregated RSSI movement recalculation trigger threshold. Enter a threshold value between 0-127 dBm. Modify only under Cisco TAC personnel guidance. **Note** When tags do not move and are being tracked, the telemetry information such as temperature will not get forwarded to the tag engine. If you do not want the tags to move but still want the notification to get forwarded, you must set the Aggregated RSSI change threshold value to zero.
Many new RSSI change percentage threshold	This parameter specifies Many new RSSI movement recalculation trigger threshold in percentage. Modify only under Cisco TAC personnel guidance.
Notification Parameters	
Rate Limit	Enter the rate, in milliseconds, at which the mobility services engine generates notifications. A value of 0 (default) means that the mobility services engine generates notifications as fast as possible (Northbound notifications only).
Queue Limit	Enter the event queue limit for sending notifications. The mobility services engine drops any event above this limit. Default values: Cisco 3350 (30000), Cisco 3310 (5,000), and Cisco 2710 (10,000).
Retry Count	Enter the number of times to generate an event notification before the refresh time expires. This parameter can be used for asynchronous transport types which do not acknowledge the receipt of the notification and there is a possibility that the notification may be lost in transit. The default value is 1. **Note** The mobility services engine does not store events in its database.
Refresh Time	Enter the wait time, in minutes, that must pass before a notification is resent. For example, if a device is configured for In Coverage Area notification and it is constantly being detected within the Coverage Area. The notification is sent once every refresh time. Default value is 0 minutes.
Drop Oldest Entry on Queue Overflow	(Read-only). The number of event notifications dropped from the queue since startup.

Field	Configuration Options
Serialize Events per Mac address per Destination	Select this option if you want the successive events for the same MAC address to be sent to a single destination in a serial manner.

Step 5 Click **Save**.

Configuring Notification Parameters

Adding Event Driven Notification Subscriptions

To add event driven notification subscriptions, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **Context Aware Service > Notification > Subscriptions**.
The Notification Subscription page appears.

Step 4 Click **Add Subscription**.

Step 5 Enter the subscription name.

Step 6 Choose the subscription type as Event Driven from the drop-down list.

Step 7 Choose the required data format from the drop-down list.

Step 8 Choose HTTP or TCP from the receiver transport drop-down list.
If you choose HTTP, you should:

1. Enter the URL.
2. Select HTTPS check box if you want to use HTTPS protocol for secure access to the destination system.

Step 9 Enter the receiver host address.

Step 10 Enter the port number of the receiver host.

Step 11 Select the Scramble MAC addresses checkbox.

Step 12 Choose the notification triggers from the drop-down list.

Step 13 Click **Save**.

Adding Streaming Notification Subscriptions

To add streaming notification subscriptions, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **Context Aware Service > Notification > Subscriptions**.
The Notification Subscription page appears.

Step 4 Click **Add Subscription**.

Step 5 Enter the subscription name.

Step 6 Choose the subscription type as streaming from the drop-down list.

Step 7 Choose the required data format from the drop-down list.

Step 8 Choose HTTP or TCP from the receiver transport drop-down list.
If you choose HTTP, you should:

1. Enter the URL.
2. Select HTTPS check box if you want to use HTTPS protocol for secure access to the destination system..

Step 9 Enter the receiver host address.

Step 10 Enter the port number of the receiver host.

Step 11 Select the Scramble MAC addresses checkbox.

Step 12 Choose the streaming type form the drop-down list.
If you choose Raw Location or RSSI Measurements, you should:

1. Choose the event entity from the drop-down list.
2. You can add /remove entity filter.

Step 13 Click **Save**.

Viewing Notification Statistics

You can view the notification statistics for a specific mobility engine. To view notification statistics information for a specific mobility services engine, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 Choose **Context Aware Service** > **Notifications** > **Statistics** to display the configuration options.
The following table lists the Notification Statistics page fields.

Table 6: Notification Statistics Page

Field	Description
Summary	
Destinations	
Total	Destinations total count.
Unreachable	Unreachable destinations count.
Notification Statistics Summary	
Destination IP Address	The destination IP address to which the notifications are sent.
Destination Port	The destination port to which the notifications are sent.
Destination Type	The type of the destination. Example: SOAP_XML.
Destination Status	Status of the destination device. The status is either Up or Down.
Last Sent	The date and time at which the last notification was sent to the destination device.
Last Failed	The date and time at which the notification had failed.
Track Definition Status	Status of the track definition. Track notification status can be either Enabled or Disabled.
Total Count	The total count of notifications sent to the destination. Click the count link to view the notification statistics details of the destination device.

Configuring Qualcomm PDS

To configure qualcomm PDS, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 From the left sidebar menu, choose **Mobile Concierge > Qualcomm Config**.
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 .

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.

Enabling Mobile Applications

To enable integration of mobile applications, follow these steps:

Step 1 Launch the MSE admin UI.

Step 2 Click the Configuration icon on the top right of the home page.

Step 3 From the left sidebar menu, choose **Mobile Concierge > Mobile App Enablement**.

Step 4 Select the **Enable Mobile App Integration** check box to enable the mobile application integration.

Step 5 Click **Save**.