CHAPTER 4

# Modifying Location Service Properties

This chapter describes how to configure location server properties.

This chapter contains the following sections:

## Modifying General Properties

You can use Cisco WCS to edit the general properties of location servers registered in the WCS database. You can edit the following general properties: contact name, user name, password and HTTPS.

To edit the general properties of a location server, follow these steps:

**Step 1** In Cisco WCS, click **Mobility > Mobility Service Engine** to display the All Servers window.

**Step 2** Click the name of the location server you want to edit.

**Step 3** At the General panel, modify the server parameters as appropriate. Table 4-1 describes each parameter.

*Table 4-1 General Properties*

| Parameter | Configuration Options |
|---|---|
| Contact Name | Enter a contact name for the location server. |
| User Name | Enter the login username for the Cisco WCS server that manages the location server. |
| Password | Enter the login password for the Cisco WCS server that manages the location server. |
| HTTPS | Check the **Enable** check box to enable HTTPS.<br>Uncheck the HTTPS enable check box to disable HTTPS. HTTP is supported by default. |

**Step 4** Click **Save** to update the Cisco WCS and location server databases.

# Editing Tracking Parameters

The location appliance can track up to 2,500 elements. You can track the following elements: client stations, active asset tags and rogue clients and access points.Updates on the locations of elements being tracked are provided to the location server from the Cisco wireless LAN controller.

Only those elements designated for tracking by the controller are viewable in Cisco WCS maps, queries and reports. No events and alarms are collected for non-tracked elements and they are not used in calculating the 2,500 element limit.

You can modify the following tracking parameters using Cisco WCS:

- Enable and disable which element locations (client stations, active asset tags, and rogue clients and access points) you actively track.
- Set limits on how many of a specific element you want to track.

  For example, given a limit of 2,500 trackable units, you could set a limit to track only 1,500 client stations. Once the tracking limit is met, the number of elements not being tracked is summarized on the Tracking Parameters page.
- Disable tracking and reporting of ad hoc rogue clients and access points.

To configure tracking parameters for a location appliance, follow these steps:

**Step 1** In Cisco WCS, click **Mobility > Mobility Service Engines**. The All Servers window appears.

**Step 2** Click the name of the location server whose properties you want to edit. The General Properties window appears.

**Step 3** In the Location menu (left panel), select **Tracking Parameters** from the Administration sub-heading to display the configuration options.

**Step 4** Modify the tracking parameters as appropriate. Table 4-2 describes each parameter.

:

*Table 4-2 Tracking and SNMP Parameters*

| Parameter | Configuration Options |
|---|---|
| Tracking Parameters | |
| Client Stations | 1. Check the **Enable** check box to enable tracking of client stations by the location server.<br>2. Check the **Enable Limiting** check box to set a limit on the number of client stations to track.<br>3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 2,500 which is the maximum number of elements tracked by a location server.<br>**Note** Active Value (display only): Indicates the number of client stations currently being tracked.<br>**Note** Not Tracking (display only): Indicates the number of client stations beyond the limit. |
| Asset Tags | 1. Check the **Enable** check box to enable tracking of asset tags by the location server.<br>2. Check the **Enable Limiting** check box to set a limit on the number of asset tags stations to track.<br>3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 2,500 which is the maximum number of elements tracked by a location server.<br>**Note** Active Value (display only): Indicates the number of asset tags currently being tracked<br>**Note** Not Tracking (display only): Indicates the number of asset tags beyond the limit. |
| Rogue Clients and Access Points | 1. Check the **Enable** check box to enable tracking of rogue clients and asset points by the location server.<br>2. Check the **Enable Limiting** check box to set a limit on the number of rogue clients and asset tags stations to track.<br>3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 2,500 which is the maximum number of elements tracked by a location server.<br>**Note** Active Value (display only): Indicates the number of rogue clients and asset tags currently being tracked.<br>**Note** Not Tracking (display only): Indicates the number of rogue clients and asset tags beyond the limit. |
| Exclude Ad-Hoc Rogues | Check 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 WCS maps or its events and alarms reported. |

*Table 4-2 Tracking and SNMP Parameters (continued)*

| Parameter | Configuration Options |
|---|---|
| SNMP Parameters | |
| SNMP Retry Count | Enter the number of times to retry a polling cycle. Default value is 3. Allowed values are from 1 to 99999.(Configurable in controller release 4.1 and earlier and location server release 3.0 and earlier only). |
| SNMP Timeout | Enter the number of seconds before a polling cycle times out. Default value is 5. Allowed values are from 1 to 99999. (Configurable in controller release 4.1 and earlier and location server release 3.0 and earlier only). |
| Client Stations | Check the **Enable** check box to enable client station polling and enter the polling interval in seconds. Default value is 300. Allowed values are from 1 to 99999. (Configurable in controller release 4.1 and earlier and location server release 3.0 and earlier only). |
| Asset Tags | Check the **Enable** check box to enable asset tag 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 and location server release 3.0 and earlier only).<br>**Note** Before the location server can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command **config rfid status enable** on the controllers. |
| Rogue Clients and Access Points | Check the **Enable** check box to enable rogue access point polling and enter the polling interval in seconds. Default value is 600. Allowed values are from 1 to 99999. (Configurable in controller release 4.1 and earlier and location server release 3.0 and earlier only). |
| Statistics | Check the **Enable** check box to enable statistics polling for the location server, and enter the polling interval in seconds. Default value is 900. Allowed values are from 1 to 99999. (Configurable in controller release 4.1 and earlier and location server release 3.0 and earlier only). |

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

# Editing Filtering Parameters

In Cisco WCS, you can limit the number of asset tags, clients, and rogue clients and access points whose whose location is tracked by filtering on:

- 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 from the WCS GUI window.

  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 noted below:

  - 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 below is a wildcard.

**Note** Allowed MAC address formats are viewable from the Filtering Parameters configuration window. See Table 4-3 for details.

  EXAMPLE file listing:

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

- Probing clients

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

To configure filtering parameters for a location appliance, follow these steps:

**Step 1** In Cisco WCS, click **Mobility > Mobility Service Engines**. The All Servers window appears.

**Step 2** Click the name of the location server whose properties you want to edit. The General Properties window appears.

**Step 3** From the **Location** menu (left panel), select **Filtering Parameters** from the Administration sub-heading to display the configuration options.

**Step 4** Modify the filtering parameters as appropriate. Table 4-3 describes each parameter.

*Table 4-3 Filtering Parameters*

| Parameter | Configuration Options |
|---|---|
| Exclude Probing Clients | Check the check box to prevent location calculation of probing clients. |
| Enable Location MAC Filtering | **1.** Check the check box to enable MAC filtering of specific elements by their MAC address.<br>**2.** To import a file of MAC addresses (*Upload a file for Location MAC Filtering* field), browse for the file name 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.<br>**Note** To view allowed MAC address formats, click on the red question mark next to the *Upload a file for Location MAC Filtering* field.<br>**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.<br>**Note** To move an address between the Allow and Disallow columns, highlight the MAC address entry and click the button under the column.<br>**Note** To move multiple addresses, click the first MAC address and depress the **Ctrl** key to highlight additional MAC addresses. Click **Allow** or **Disallow** to transfer it to the MAC address to its destination.<br>**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 location server database.

# Editing History Parameters

You can use Cisco WCS to specify how often to collect client station, rogue access point, and asset tag histories from the controllers associated with a location server.

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

To configure location server history settings, follow these steps:

**Step 1** In Cisco WCS, click **Mobility > Mobility Service Engines**. The All Servers window appears.

**Step 2** Click the name of the location server whose properties you want to edit.

**Step 3** From the **Location** menu (left panel), select **History Parameters** from the Administration sub-heading to display the configuration options.

**Step 4** Modify the following history parameters as appropriate. Table 4-4 describes each parameter.

:

*Table 4-4 History Parameters*

| Parameter | Configuration Options |
|---|---|
| Archive for | Enter the number of days for the location server to retain a history of each enabled category. Default value is 30. Allowed values are from 1 to 99999. |
| Prune data starting at | Enter the interval of time in which the location server starts data pruning (between 0 and 23 hours, and between 1 and 59 minutes). Also enter the interval in minutes after which data pruning starts again (between 0, which means never, and 99900000). Default start time is 23 hours and 50 minutes, and the default interval is 1440 minutes. |
| Client Stations | Check the **Enable** check box to turn historical data collection on for client stations, and enter the number of minutes that elapse between data collection events. Default value is 120. Allowed values are from 1 to 99999. |
| Asset Tags | Check the **Enable** check box to turn historical data collection on for asset tags, and enter the number of minutes that elapse between data collection events. Default value is 180. Allowed values are from 1 to 99999.<br>**Note** Before the location server can collect asset tag data from controllers, you must enable the detection of RFID tags using the CLI command **config rfid status enable**. |
| Rogue Clients and Access Points | Check the **Enable** check box to turn historical data collection on for rogue clients and access points, and enter the number of minutes between data collection events. Default value is 360. Allowed values are from 1 to 99999. |

*Table 4-4 History Parameters (continued)*

| Parameter | Configuration Options |
|---|---|
| Wired Stations | Check the **Enable** check box to turn historical data collection on for wired stations, and enter the number of minutes between data collection events. Default value is 720. Allowed values are from 1 to 99999. |
| Enable History Logging of Location Transitions for *Client Stations, Asset Tags* and *Rogue Clients and Access Points* | Check any or all of the client stations, asset tags or rogue clients and access points check boxes to log location transitions. When history logging is enabled for an element, a location transition event is logged each time the location of the selected element changes. |

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

# Editing Location Parameters

You can use Cisco WCS to modify parameters that affect location calculation such as Receiver Signal Strength Indicator (RSSI) measurements.

You can also apply varying smoothing rates to manage location movement of an element.

To configure advanced location parameters, follow these steps:

**Step 1** In Cisco WCS, click **Mobility> Mobility Service Engine**.

**Step 2** Click the name of the location server whose properties you want to edit.

**Step 3** From the **Location** menu (left panel), select **Location Parameters** from under the Advanced sub-heading. The configuration options appear.

**Step 4** Modify the location parameters as appropriate. Table 4-5 describes each parameter.

*Table 4-5 Location Parameters*

| Parameter | Configuration Options |
|---|---|
| Calculation time | Check the corresponding check box to enable the calculation of the time required to compute location.<br>⚠ **Caution** Enable only under Cisco TAC personnel guidance because enabling this parameter slows down overall location calculations. |
| OW Location | Check the corresponding check box to enable Outer Wall (OW) calculation as part of location calculation.<br>**Note** The OW Location parameter is ignored by the location server. |

*Table 4-5 Location Parameters (continued)*

| Parameter | Configuration Options |
|---|---|
| Relative discard RSSI time | Enter the number of minutes since the most recent RSSI sample after which RSSI measurement should be considered stale and discarded. For example, if you set this parameter to 3 minutes and the location server receives two samples at 10 and 12 minutes, it keeps both samples. An additional sample received at 15 minutes is discarded. Default value is 3. Allowed values range from 0 to 99999. *A value of less than 3 is not recommended.* |
| Absolute discard RSSI time | Enter the number of minutes after which RSSI measurement should be considered 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.* |
| RSSI Cutoff | Enter the RSSI cutoff value, in decibels (dBs) with respect to one (1) mW (dBm), above which the location server will always use the access point measurement. Default value is –75.<br>**Note** When 3 or more measurements are available above the RSSI cutoff value, the location server will discard any weaker values and use the 3 (or more) strongest measurements for calculation; however, when only weak measurements below the RSSI cutoff value are available, those values are used for calculation.<br>**Caution** Modify only under Cisco TAC personnel guidance. Modifying this value can reduce the accuracy of location calculation. |
| Smooth Location Positions | Smoothing compares an elements prior location to its most recent reported location by applying a weighted average calculation to determine its current location. The specific weighted average calculation employed is tied to the given smoothing option selected. Default value is More Smoothing.<br>Options:<br>• Off (No smoothing): Elements assumed to be in location indicated by most recent polling<br>• Less smoothing: Prior location weighted at 25% and New location weighted at 75%<br>• Average smoothing: Prior location weighted at 50% and New location weighted at 50%<br>• More smoothing: Prior location weighted at 75% and New location weighted at 25%<br>• Maximum smoothing: Prior location weighted at 90% and New location weighted at 10% |
| Chokepoint Usage | Check the Enable check box to enable tracking of Cisco compatible tags by chokepoints. |

*Table 4-5 Location Parameters (continued)*

| Parameter | Configuration Options |
|---|---|
| Use Chokepoints for Interfloor conflicts | Perimeter chokepoints or weighted location readings can be selected to determine the location of Cisco compatible tags.<br>Options:<br>• Never: When selected, perimeter chokepoints are not used to determine the location of Cisco compatible tags.<br>• Always: When selected, perimeter points are used to determine the location of Cisco compatible tags.<br>• Floor Ambiguity: When selected, both weighted location readings and perimeter chokepoints are used to generate location for 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. |
| Allow Civic Address updates from Switches | Check the **enable** check box to receive civic address updates from the controller. When enabled, the civic address parameter provides city, state, postal code and country specifics for the location appliance. This capability is in addition to the Cisco default settings of campus, building, floor, and X, Y coordinates. This information can then be requested by clients on demand for use by location-based services and applications.<br>**Note** For more details on civic addresses and other location options, refer to the“Enabling Location Presence on a Location Server” section on page 7-24. |

**Step 5** Click **Save** to store your selections in the Cisco WCS and location server databases.

# Editing NMSP Parameters

In releases 3.1 and later, the Network Mobility Services Protocol (NMSP) manages communication between the location server and the controller.

**Note** In location server release 3.0, the location protocol (LOCP), now identified as NMSP, transported telemetry, emergency, and chokepoint information between the location server and the controller. All other information was transmitted using SNMP polling. Releases prior to 3.0 did not support LOCP and updates between the controller and the location server solely used SNMP polling.

**Note**

- The NMSP parameter is supported in location servers installed with release 3.0 or greater.
- NMSP replaces the LOCP term introduced in release 3.0.
- Telemetry, emergency and chokepoint information is only seen on controllers and Cisco WCS installed with release 4.1 software or greater and on location servers running release 3.0 or greater software.
- The TCP port (16113) that the controller and location server communicate over MUST be open (not blocked) on any firewall that exists between the controller and location server for NMSP to function.

To configure NMSP parameters, follow these steps:

**Step 1** In Cisco WCS, click **Mobility> Mobility Service Engine**.

**Step 2** Click the name of the location server whose properties you want to edit.

**Step 3** From the **Location** menu (left panel), select **NMSP Parameters** from the Advanced sub-heading. The configuration options appear.

**Step 4** Modify the NMSP parameters as appropriate. Table 4-6 describes each parameter.

**Note** No change in the default parameter values is recommended unless the network is experiencing slow response or excessive latency.

*Table 4-6 NMSP Parameters*

| Parameter | Configuration Options |
|---|---|
| Echo Interval | Defines how frequently an echo request is sent from a location server to a controller. The default value is 15 seconds. Allowed values range from 1 to 120 seconds.<br>**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 location server waits for a successful echo response from the controller before declaring the neighbor dead. This timer begins when the echo request is sent.<br>The default value is 30 seconds. Allowed values range from 1 to 240 seconds.<br>**Note** This value must be at least two times the echo interval value. |
| Response Timeout | Indicates how long the location server waits before considering the pending request as timed out. The default value is 1 second. Minimum value is one (1). There is no maximum value. |

*Table 4-6 NMSP Parameters (continued)*

| Parameter | Configuration Options |
|---|---|
| Retransmit Interval | Interval of time that the location server 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 set 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 Cisco WCS and location server databases.