Enhanced Location Tracking For Jabber Clients

- Enhanced Location Tracking for Jabber Clients, on page 1
- Enhanced Location Tracking Recommendations Considerations, on page 2
- Initial Configurations for Enhanced Location Tracking for Jabber Clients, on page 3
- Configure Access Points in Unified Communications Manager, on page 4
- Configure Cisco Jabber on Unified Communications Manager, on page 6
- Configure Cisco Jabber Configuration Files in Unified Communications Manager, on page 6
- Configure AXL Application User, on page 7
- Enable Change Notifications, on page 8
- Configure Access Points in Cisco Emergency Responder, on page 8
- Set Up SNMP Connection, on page 8
- Configure AXL Application User for Emergency Responder, on page 10
- Assign ERLs, on page 12
- Configure AXL Phone Tracking, on page 12
- Troubleshooting Enhanced Location Tracking For Jabber Clients, on page 13

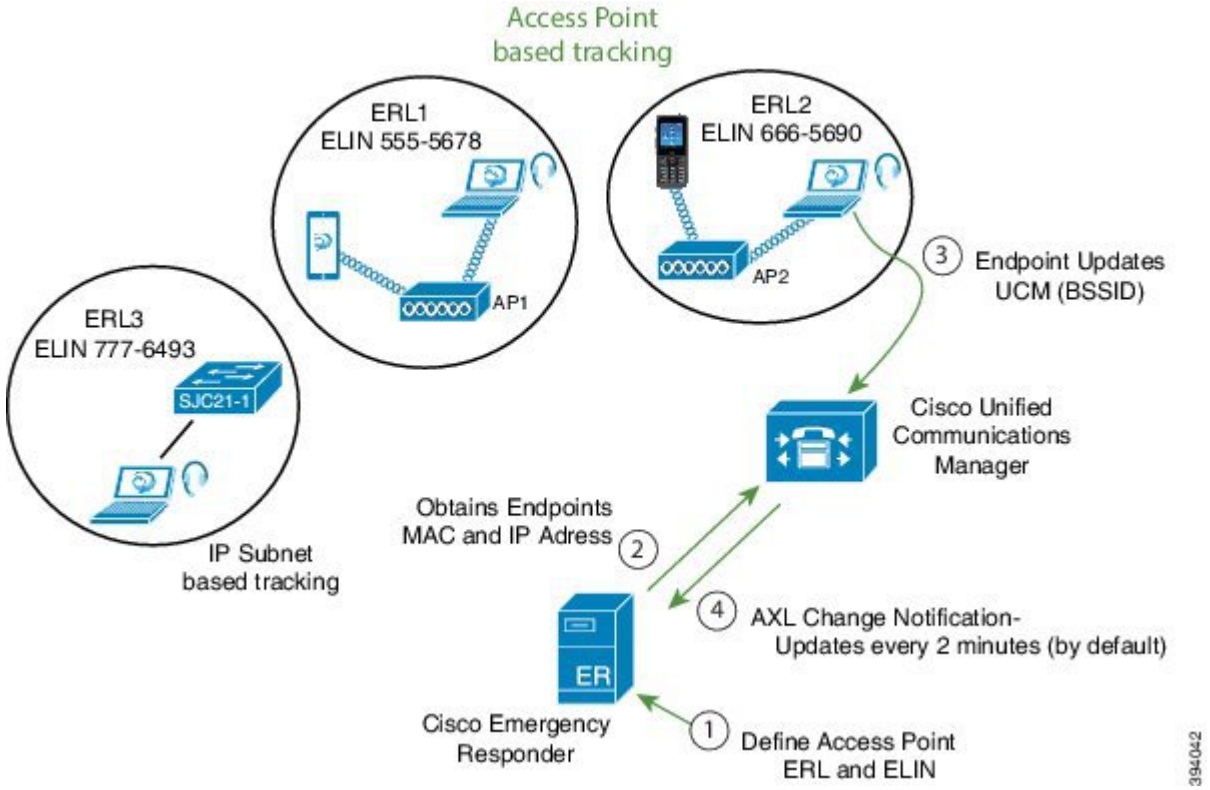
Enhanced Location Tracking for Jabber Clients

The Enhanced Location Tracking allows Unified Communications Manager along with Emergency Responder tracks the physical location of wireless Cisco Jabber clients. The location is tracked through a wireless access point which serves as the location identifier.

Unified Communications Manager can synchronize all the wireless access points deployed in the infrastructure through a Wireless LAN Controller (WLC) synchronization or through a manual import using Bulk Administration Tool (BAT). Using AXL discovery, the Emergency Responder administrators can learn about the various access points through the Unified Communications Manager. The Emergency Responder administrator defines emergency response locations (ERLs) for these access points and corresponding 911 call treatment. Cisco Jabber clients, if defined by the Policy in Unified Communications Manager, sends their upstream infrastructure information like BSSID and any subsequent changes to Emergency Responder. Emergency Responder provides ERL treatment to Cisco Jabber clients based on the associated access point.

Note Emergency Responder AXL discovery runs every 2 minutes (by default) to identify a location update (Access Point BSSID) and so can be identified within 2 to 4-min period. If the system is running large number of Jabber clients or load conditions, administrators can change the frequency accordingly. Any AXL communication error is reported through the Event Viewer and the administrator must take corrective actions immediately.

Figure 1: Basic Deployment of Enhanced Location Tracking



Enhanced Location Tracking feature is available for the following components:

- Unified Communications Manager Release 12.5.1SU1
- Emergency Responder 12.5.1SU1
- Cisco Jabber 12.6

Enhanced Location Tracking Recommendations Considerations

- Enhanced location tracking feature works only for the 12.5.1SU1 or above versions of Emergency Responder and Unified Communications Manager.
- If any Cisco Jabber or wireless device falls under non-defined Access Points, then the device is tracked using IP subnet (if IP subnet is configured) or Unlocated Phones page.

- Cisco Jabber devices should be tracked using the AXL discovery method. The MAC address of a Cisco Jabber device (wireless or wired) displays the same details as the Device Name.
- Off-Premise emergency response location (ERL) does not support Cisco Jabber AXL discovery tracking.
- Emergency Responder Clustering is not supported. Phones that are discovered using AXL discovered phones is not shared through an Emergency Responder cluster.
- If different Unified Communications Manager clusters are connected to Emergency Responder, you should not use the combination of different Unified Communications Manager versions. For example, you should not combine a Release 12.5.SU1 Unified Communications Manager with a version above or below. Similarly, if multiple clusters of Unified Communications Manager are connected to Emergency Responder, then all the Unified Communications Manager clusters should have release 12.5.1SU1 version or above.
- For enhanced location tracking, if the Unified Communications Manager version is over 12.5.1SU1 release and above, different discoveries take the following priority:
  - If Major discovery is running, AXL discovery and phone tracking cannot take place.
  - If Incremental discovery is running, AXL discovery can run in parallel.

Initial Configurations for Enhanced Location Tracking for Jabber Clients

The following sections describe the initial setup tasks that you must complete before you begin to configure the enhanced location tracking feature for Cisco Jabber devices.

- Unified Communications Manager Configurations Task Flow, on page 3
- Emergency Responder Configurations Task Flow, on page 4

Unified Communications Manager Configurations Task Flow

Perform the following tasks to set up your access points in Unified Communications Manager.

Procedure

	Command or Action	Purpose
Step 1	Configure Access Points in Unified Communications Manager, on page 4	Use the instructions in this task to synchronize the database with a Cisco Wireless Access Point Controller (WLC) use either of the following tasks: • Through a Wireless LAN Controller (WLC). • Inserting a CSV file into the Unified Communications Manager database.

	Command or Action	Purpose
Step 2	Configure Cisco Jabber on Unified Communications Manager, on page 6	Adds a Cisco Jabber device manually.
Step 3	Configure Cisco Jabber Configuration Files in Unified Communications Manager, on page 6	Creates Jabber Client Configuration (jabber-config.xml) files and associates them to end users.
Step 4	Configure AXL Application User, on page 7	Use this procedure to configure an AXL user that Emergency Responder uses to access the device configuration and database access.
Step 5	Enable Change Notifications, on page 8	Use this procedure to enable AXL change notifications in support for the Enhanced Location Tracking feature.

Emergency Responder Configurations Task Flow

Perform the following procedures to provision the access points and track Cisco Jabber devices (wired or wireless) that are configured in Unified Communications Manager and discovered by Emergency Responder.

Procedure

	Command or Action	Purpose
Step 1	Set Up SNMP Connection	Emergency Responder uses SNMP to obtain information about Unified Communications Manager nodes in the cluster.
Step 2	Configure AXL Application User, on page 7	You must configure the AXL application user for Emergency Responder on Unified Communications Manager.
Step 3	Set Up Default ERL	You can create emergency response locations (ERLs) for tracking devices under a single location.
Step 4	Configure AXL Phone Tracking, on page 12	Use this procedure to track wired or wireless Cisco Jabber devices from any location.

Configure Access Points in Unified Communications Manager

There are two types of deployment models for Access Points configuration:

- Configure Access Points Through Wireless LAN Controller Synchronization Service, on page 5
- Configure Access Points Using Bulk Administration Tool, on page 5

Configure Access Points Through Wireless LAN Controller Synchronization Service

To configure access points through WLAN Controller, use the following procedure:

Procedure

Step 1 In the Cisco Unified Serviceability interface, choose **Tools > Service Activation** and select the publisher node.

Step 2 From the Location based Tracking Services, check the **Cisco Wireless Controller Synchronization Service** option and save the configuration changes. This will activate the CWLCSS service.

Step 3 In Cisco Unified Serviceability interface, choose **Tools > Control Centre – Feature Services**.

Step 4 Select the publisher node to enable the **Cisco Wireless Controller Synchronization Service** option from the Location based Tracking Services section.

Step 5 In Cisco Unified CM Administration user interface, choose **Advanced Features > Device Location Tracking Services > Wireless Access Point Controllers**.

Step 6 Enter the required details in **Wireless Access Controller Details** and select an automatic synchronization schedule using the **Wireless Access Point Controller Synchronization Schedule**. Click **Save**.

Step 7 After synchronizing a WLC, in Cisco Unified CM Administration user interface, navigate to **Advanced Features > Device Location Tracking Services > Switches and Access Points** to view all the access points details.

Configure Access Points Using Bulk Administration Tool

An IPv4 address, IPv6 address, or BSSID may be associated with only one infrastructure device. Two devices cannot have the same IP address or BSSID. Also, all BSSIDs must end in 0.

Before you begin

Create a .csv file with the following delineated columns: ACCESS POINT or SWITCH NAME, IPV4 ADDRESS, IPV6 ADDRESS, BSSID, DESCRIPTION.

Procedure

Step 1 In Cisco Unified CM Administration user interface, navigate to **Bulk Administration > Upload/Download files** and upload the .csv file.

Step 2 Choose **Bulk Administration > Infrastructure Device > Insert Infrastructure**.

Step 3 In the **File Name** field, choose the CSV data file that you created for this transaction.

Step 4 In the **Job Information** area, enter the job description.

Step 5 Choose the .csv file and select the option **Run Immediately** or **Run Later** as per the requirement. If you choose to **Run Later**, ensure you use the Job Scheduler page to schedule and activate the job.

Step 6 Click **Submit**.

Step 7 To verify whether your device is added, navigate to **Advanced features > Device Location Tracking services > Switches and Access Points**.

You can view all the Access Points that were successfully added through the Bulk Import.

Configure Cisco Jabber on Unified Communications Manager

Note Ensure that you specify the name of the Jabber device configuration type (CSF, BOT, TCT, or TAB) in the **Device Name** of the Phone Configuration window.

To add a new Cisco Jabber device manually with a user, perform the following procedure:

Procedure

Step 1 From the Cisco Unified CM Administration, choose **Device > Phone > Add a New Phone**.

Step 2 From Find and List Phones page, click **Add New** to manually add a phone.

Step 3 Find and select the appropriate wireless or Jabber device which you want to add to your access point.

Step 4 Complete the fields in the **Phone Configuration** window.

Step 5 Click **Save**.

Step 6 If you want to add another Cisco Jabber device, repeat these steps.

Configure Cisco Jabber Configuration Files in Unified Communications Manager

The following are three new configuration parameters that must be set to have the Jabber client send location updates:

- EnableE911OnPremLocationPolicy
- EnableE911EdgeLocationPolicy
- 911EdgeLocationWhiteList

For more information on the parameters, see https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/12_5/Parameter_Guide/cjab_b_parameters-reference-guide-jabber_125.html.

If these three parameters are not properly configured, then by default, Jabber will not send the location updates. You can centrally manage Jabber client configuration parameters using the Cisco Unified CM Administration interface. You can create multiple Jabber Client Configuration templates for various deployment scenarios and assign them to end users. Jabber clients can now send their location information to Unified Communications Manager.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface on Unified Communications Manager.

Step 2 Select **User Management > User Settings > UC Service**.

Step 3 Using the **Jabber Client Configuration (jabber-config.xml)** service, you can create multiple Jabber Client Configuration templates as per your deployment needs.

Note Ensure that you configure the three new configuration parameters for Cisco Jabber device tacking.

Step 4 Navigate to **User Settings > Service Profiles** to associate them to Common, Desktop, and Mobile Jabber client types once the templates are created.

Step 5 Navigate to **User Management > End User** to add a new user.

Step 6 Select a **UC Service Profile** that you have created in Step 3 for this end user.

Configure AXL Application User

Note It is not mandatory that CallManager Service runs on all Unified Communications Manager nodes. Only the Unified Communications Manager that is configured in Emergency Responder and the Unified Communications Manager nodes that acts as the backup server (in case of connection failures) needs to run the CallManager Service.

To create a new AXL application user, perform the following procedure:

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management > Application User**.

Step 2 Click **Add New** to create a new application user and configure the fields in the Application User Configuration window.

Step 3 Click **Save**.

Step 4 In Cisco Unified CM Administration, choose **User Management > User Settings > Role**.

Step 5 Click **Add New** and select **Cisco CallManager AXL Database** and configure the remaining fields.

Step 6 Ensure that you check the **Allow to use API** check box and click **Save**.

Step 7 In Cisco Unified CM Administration, choose **User Management > User Settings > Access Control Group**.

Step 8 Click **Add New**, enter a name and click **Save**.

Step 9 Click **Add App User to Group**.

Step 10 Search for the user with the new application User ID, check the required check box to select the user and click **Add Selected**.

Step 11 Select **Assign Role to Access Control Group** from the drop-down list on the top right side.

Step 12 Click **Assign Role to Group** and select **Custom AXL Access** to select the role.

Step 13 Click **Add Selected** and save the configuration changes.

Enable Change Notifications

Procedure

Step 1 In Cisco Unified CM Administration user interface, navigate to **System > Service Parameter**.

Step 2 Select the publisher server and select **Cisco Database Layer Monitor (Active)**.

Step 3 Click **Advanced**.

Step 4 Under Clusterwide Parameters section, make sure that the parameter value of **AXL Change Notification** is set to On and click **Save**.

Configure Access Points in Cisco Emergency Responder

Perform the following procedures to provision the access points and track Cisco Jabber devices (wired or wireless) that are configured in Unified Communications Manager and discovered by Emergency Responder:

- Set Up SNMP Connection
- Configure AXL Application User for Emergency Responder, on page 10
- Assign ERLs, on page 12
- Configure AXL Phone Tracking, on page 12

Set Up SNMP Connection

Emergency Responder uses SNMP to obtain information about the ports on a switch. Emergency Responder must obtain this port information so that you can assign the ports to ERLs, and so that Emergency Responder can identify phones that are attached to the ports and update their ERL assignments.

Emergency Responder only reads SNMP information, it does not write changes to the switch configuration, so you only have to configure the SNMP read community strings.

When you configure the SNMP strings for your switches, you must also configure the SNMP strings for your Unified CM servers. Emergency Responder must be able to make SNMP queries of all Unified CM servers in the cluster that it supports.

If your Cisco Emergency Responder servers, Unified CM servers, and Cisco IP Phones are in a different subnet than your switches, you must either configure both the subnets for the servers and phones as well as the subnet for the switches or use *.*.*.*.

Related Topics

SNMP Settings

LAN Switch Identification

Set Up SNMP Community String

By configuring SNMP, you can control SNMP access to the Emergency Responder SNMP agent. A management station must first submit a valid community string for authentication.

You configure a community string by entering the Community String Name, the IP addresses of host that can be authenticated using the community string, and the access privileges allowed. The available access privileges are as follows:

- ReadOnly
- ReadWrite
- ReadWriteNotify
- NotifyOnly
- None

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **SNMP > V1/V2C Configuration > Community String**.
The SNMP Community String Configuration page appears.

Step 2 Enter the name of the community string in the Community String Name text box.

Step 3 Click **Accept SNMP Packets only from these hosts** to specify specific hosts whose SNMP packets will be accepted, enter the IP addresses in the text box, and click **Insert**.

To accept SNMP packets from any host, click the **Accept SNMP Packets from any host** radio button.

Step 4 Select the host IP address and click **Remove** to remove an existing host, .

Step 5 Select the access privilege for the host from the Access Privileges pull-down menu then click **Insert**.

Related Topics

SNMP Community String Configuration

Set Up SNMP Users

SNMP V3 provides additional security features that include message integrity, authentication, and encryption. In addition, SNMP V3 controls user access to specific areas of the MIB tree.

Note FIPS Mode and Enhanced Security Mode do not support MD5 or DES encryption methods. If SNMPv3 setting is enabled using MD5 or DES, then enabling FIPS Mode or Enhanced Security Mode changes these encryption methods to SHA-1 or AES-128 respectively.

Before Emergency Responder (in FIPS Mode) upgrade, ensure that there are no MD5 or DES encryption methods in the FIPS Mode. If the MD5 or DES encryption methods were not updated to SHA-1 or AES-128 respectively in the FIPS Mode before upgrade, they will get updated automatically after the upgrade.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, choose **SNMP** > **V3 Configuration** > **User**.

Step 2 Click **Add New** to add a new SNMP User.

Step 3 Enter the new SNMP user name in the **User Name** text box.

Step 4 Check the **Authentication Required** check box to require authentication. Enter a password in the **Password** text box, reenter the password in the **Reenter Password** textbox, and choose either **MD5** or **SHA** to select an authentication protocol. Click **Insert** to add the user.

Step 5 Check the **Privacy Required** check box to require information privacy. Enter a password in the **Password** textbox, reenter the password in the **Reenter Password** textbox, and choose either **DES** or **AES** to select a privacy protocol.

Note A message appears to restart the SNMP master agent for the changes to take effect. Click **OK** to restart the SNMP master agent or **Cancel** to continue without restarting the master agent.

The new user is added to the list of users on the SNMP User Configuration page.

Step 6 Repeat Step 2 through to Step 4 to add additional users.

Related Topics

SNMP User Configuration

Set Up MIB2

The SNMP MIB2 tool allows you to specify a contact person for a MIB2 managed node and the physical location of the managed node.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **SNMP > System Group Configuration > MIB2 System Group Configuration**.

Step 2 In the **System Contact** text box, enter the name of the contact.

Step 3 In the **Location** text box, enter the location of the managed node.

Step 4 Click **Update** in the upper left corner of the page.

Step 5 Click **Clear** in the upper left corner of the page to modify the information, enter the new information in the **System Contact** and **Location** text boxes, and click **Update**.

Related Topics

MIB2 System Group Configuration

Configure AXL Application User for Emergency Responder

You must configure the AXL application user for Emergency Responder on Unified Communications Manager, so that an off-premises user can log in to the Emergency Responder off-premises user website.

Note You should use the Unified Communications Manager release 12.51SU1 version to locate Cisco Jabber through AXL application.

Procedure

Step 1 In CiscoUnifiedCM Administration interface, choose **User Management > Application User**. Click **Add New**.

Step 2 Complete the following required fields:

- **User ID**—Use a descriptive name such as AXL Application User.
- **Password**—Enter a password for this user.
- **Confirm Password**—Reenter the password for this user.

Step 3 Click **Save**.

Step 4 Choose **User Management > User Group**.

Step 5 At search criterion, enter **standard** and click **Find**.

The list of user groups starting with the name standard appears.

Step 6 Click **Standard CCM Admin Users** to display the User Group configuration page.

Step 7 Click **Add App Users to Group**.
The Find and List Application Users pop-up window appears.

Step 8 Enter the User ID created in Step 2 as the search criterion and click **Find**.
The list of Applications users appears.

Step 9 Click the check box next to the user ID. Click **Add Selected**.

Unified Communications Manager adds the selected user to the **Standard CCM Admin Users** user group.

Step 10 Choose **User Management > User Group**.
The user group search page appears.

Step 11 Enter **standard** as the search criterion and click **Find**.
The list of user groups starting with the name Standard appears.

Step 12 Click the **Standard TabSync User** group.

Step 13 Repeat steps 7 through 9 to add the user to the Standard TabSync User group.

Step 14 Choose **User Management > User Group**.
The user group search page appears.

Step 15 Enter **standard** as the search criterion and click **Find**.
The list of user groups starting with the name Standard appears.

Step 16 Click the **Standard RealtimeAndTraceCollection** group.

Step 17 Repeat steps 7 through 9 to add the user to the Standard RealtimeAndTraceCollection group.

Assign ERLs

Emergency Responder does not automatically assign new switch ports and unlocated phones to the default emergency response location (ERL). New switch ports and unlocated phones are treated as ERLs that are not configured.

You must not configure the default ERL to any of the Switch Ports, Unlocated Phones, Manually Configured Phones or IP subnets. The default ERL is used internally by Emergency Responder only if no other ERL is configured for that phone.

Emergency Responder also uses the default ERL for all emergency calls when the Emergency Responder server is first started (or restarted when there is no standby Emergency Responder server) until the initial switch port update is finished. (This process is started immediately.)

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

You must first configure the required ELINs in Unified Communications Manager.

Procedure

Step 1 Select **ERL > Conventional ERL**.

Step 2 Click **Configure Default ERL**.

Step 3 Fill in the ERL Information for Default window.

Step 4 Click **ALI Details**.

Step 5 Fill in the ALI Information window.

When finished filling in the ALI, click **Update ALI Info**. Emergency Responder saves your ALI. Click **Close** to close the window.

Step 6 Make the ERL Information for Default window the active window if it is not, and click **Update**.

Emergency Responder saves the ERL and its ALI.

Step 7 Click **Close** to close the window.

Tip You cannot delete the default ERL. In addition, you cannot configure other ERLs unless the default ERL is configured.

Configure AXL Phone Tracking

To track phones successfully, Emergency Responder must periodically contact Unified Communications Manager and switches to obtain the port and device information. Emergency Responder updates network information using two processes:

- Phone Tracking—A periodic comparison of the phones registered with Unified Communications Manager to the location information is obtained from the switches. If a phone moves, Emergency Responder updates the phone's ERL. Phones that cannot be located are classified as unlocated.

Note If you do not configure a switch port phone update schedule, the default schedule runs at midnight.

- Switch-Port and Phone Update—The phone tracking process plus a more extensive check of the network switches, which can identify new or changed switch modules (additional or removed ports). Any newly discovered ports are assigned to the Default ERL. Ensure that your ERL administrator updates the ERL assignment for new ports.

Before you begin

You must have system administrator or network administrator authority to define the schedule.

Procedure

Step 1 Select **Phone Tracking** > **Schedule**.

Step 2 Enter the incremental phone tracking schedule in minutes and click **Update**.

Emergency Responder runs the phone tracking process after this number of minutes from the start of previous phone tracking process.

Step 3 Enter the AXL incremental location phone tracking schedule in minutes and click **Update**.

Emergency Responder runs the enhanced location phone tracking for wireless devices after this number of minutes from the start of previous location tracking process.

Note By default, Emergency Responder actively queries the Cisco Jabber client every 2 minutes through AXL discovery on receipt of the device location.

Step 4 Enter the schedule for the switch port and phone update process. You should run this process at least once per day (but not more than four times per day).

Troubleshooting Enhanced Location Tracking For Jabber Clients

Unable to Discover Cisco Jabber or Access Points from Unified Communications Manager

Problem: If the AXL Change Notification queue has changed due to Unified Communications Manager reboot or upgrade, or Tomcat services restart, the server log displays the following error message: *500 internal error for the AXL request sent by CER*.

Solution: The **CER Service** needs to be restarted.

Emergency Responder Lost Connection with Unified Communications Manager

Problem: If Unified Communications Manager publisher node goes down, Emergency Responder loses connection due to queue identifier (QID) mismatch and tries to connect to another Unified Communications Manager node in the same cluster. Displays the following error message based on the AXL phone tracking schedule configured: AXL Phone Discovery failed to connect to axl url- *https://<ip address>*:8443.

Connectivity issues arise due to the following:

- AXL connection down
- AXL authentication credentials changed
- Unified Communications Manager server is rebooted
- Tomcat services restarted

Solution: Ensure that the AXL credentials are correct. If the credentials are correct, verify whether the AXL service is running on Unified Communications Manager and restart the **CER Service**.

Major Discovery Shows Message Incorrectly that Phone Tracking is in Progress

Problem: When a forced Major discovery is initiated for enhanced location tracking during ongoing AXL discovery, it displays an incorrect message stating “Phone tracking is in progress”.

Solution: Run the Major discovery after sometime.