Managing Devices in Prime Collaboration Provisioning

Managing Devices Overview

To use Cisco Prime Collaboration Provisioning, you must first add the IP communications infrastructure devices that are part of your IP telephony environment.

After adding devices, you synchronize the data in Cisco Unified Communications Manager, Cisco Unity systems, and Cisco IM and Presence with Cisco Prime Collaboration Provisioning. This populates Cisco Prime Collaboration Provisioning with the existing active users and services, and provides a consolidated view of all of the infrastructure and user information.

Provisioning also provides support for Cisco IOS routers. When a Cisco IOS router device is added to Prime Collaboration Provisioning, it appears in Cisco Prime Collaboration Provisioning as a Generic IOS Router. Through the Generic IOS Router capability, Cisco Prime Collaboration Provisioning can configure additional voice functionality on the router.

Call Processors are proxies for each instance of a Cisco Unified Communications Manager or Cisco Unified Communications Manager Express device. Unified Message Processors are proxies for each instance of a Cisco Unity Express, or Cisco Unity Connection device. Unified Presence Processors are proxies for each instance of Cisco IM & Presence. You will find these terms used in place of their respective devices.

Adding Devices

You must add devices to Cisco Prime Collaboration Provisioning to provision services for users. For a list of devices you can add to Cisco Prime Collaboration Provisioning, see Supported Devices for Prime Collaboration Provisioning.

Note the following points while you are adding a device to Cisco Prime Collaboration Provisioning:

- Before you add devices to Cisco Prime Collaboration Provisioning, you must ensure that Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, Cisco Unity Connection, Cisco Unity Express devices are configured correctly. For details on configuring these devices, see Setting Up Devices for Prime Collaboration Provisioning.
- For infrastructure devices (Cisco Unified Communications Manager, Cisco Unity Connection, and Cisco Unified Presence) that are setup in a cluster environment, add the publisher information and credentials only.
- There are some significant differences in how a Generic IOS Router is set up in Cisco Prime Collaboration Provisioning in comparison to a Cisco Unified Communications Manager or a Cisco Unity device. Most notably, Generic IOS Routers are not synchronized and they are not associated to a Domain or a Service Area.
- Before you can create a Call Processor based on a Cisco Unified Communications Manager Express in Cisco Prime Collaboration Provisioning, you must:
  - Disable the auto-allocation of directory numbers. Do this through the Cisco IOS interface.
  - Disable the ephone auto-registration for Cisco Unified Communications Manager Express.

To add devices to Provisioning:

Step 1 Choose **Device Setup**.

Step 2 In the Device Setup page, click **Add** to add devices to Cisco Prime Collaboration Provisioning.

Step 3 In the Add Device window, select the required application from the drop-down list and enter the necessary information such as Name, IP address, and so on. See the tables below for field descriptions.

Note For the device name, valid values are space, alphanumeric characters (A-Z, a-z, 0-9), underscore (_), hyphen (-), period (.), and at sign (@).

Note In case of setting a password for Cisco Unity Connection, you cannot use a semicolon as the Cisco Unity Connection Interface does not allow it.

Note To add Unity Connection versions 10.x or higher to the Cisco Prime Collaboration Provisioning Device setup page, you need to configure a proxy user on the Unity Connection server.

Step 4 (Optional) Click **Test Connection** to check the connectivity of the device with respect to name, IP address, application, version, username, and password. You can test connection without saving the device.

Note Test Connection is not supported for Deployment Manager, Prime License Manager, Expressway Edge, and Expressway Core.

Step 5 Click **Save**.

Devices are added to Cisco Prime Collaboration Provisioning. You can see two status messages appearing at the bottom of the page. One on whether the addition of the device was successful or not, and another on the Test Connection stating whether the connectivity test was successful or not. Devices with multiple applications are added as separate devices in the table.

Note While adding Cisco Unity Connection 10.0 and above versions, you must configure both Unity Connection administrator and Operating System (OS) administrator credentials.

If the Test Connection fails while adding Cisco Unity Connection 10.5.2 and above versions, first verify the connectivity of port 8081 to Cisco Unity Connection from Cisco Prime Collaboration Provisioning. If the connectivity succeeds, create a proxy user in the Cisco Unity Connection publisher. After creating a proxy user, edit the device details and update the OS Admin credentials with the new proxy user credentials.

If the Test Connection fails while adding Cisco Unity Connection 10.5.2 and above versions, first verify the connectivity of port 8081 to Cisco Unity Connection from Cisco Prime Collaboration Provisioning. If the connectivity succeeds, create a proxy user in the Cisco Unity Connection device. After creating a proxy user, edit the device details and update the OS Admin credentials with the new proxy user credentials.

To create proxy user, login as administrator in Cisco Unity Connection and enter the following CLI commands:

```
utils cuc proxy usrcreate
utils cuc proxy usrpasswd
utils cuc proxy enable
```

To view the details of the device, hover over **Quick View**. You can start synchronization, view synchronization logs, test the connectivity of the device, and cross launch Cisco Unified CM Serviceability and Cisco Unity Connection Serviceability from Quick View. The Quick view also displays the status of Jabber service (enabled from Unified Communication Services pane and Getting Started wizard) and Self-Provisioning (enabled through Getting Started wizard) for the device.

To update or change the device details, click **Edit**.

Some devices have more than one application on it (devices with same IP address). If you are adding devices with more than one application on it, add the first device and save it. After the device is successfully added to Provisioning, add the device again, selecting the second application. Save the device. Both the devices appear in the Device Setup table.

You can add Prime License Manager and Deployment Manager from the Infrastructure Setup page. After you add these devices, Prime License Manager and Deployment Manager links are displayed under the Administration menu. Click on the Prime License Manager or Deployment Manager link to cross launch the Prime License Manager or Deployment Manager login page.

Note You can add only one Prime License Manager and Deployment Manager device to Cisco Prime Collaboration Provisioning. If you try to add another Prime License Manager or Deployment Manager device, an error message is displayed.

Table 1: Call Processor Fields

Field	Description
LDAP Integration	

Field	Description
	Following are the options: • None—Select this option if you have not enabled both LDAP synchronization and authentication in Cisco Unified CM, and want to push users from Cisco Prime Collaboration Provisioning user interface onto the UC applications. **Note** For Cisco Unified CM 10.5(1) and above: • For Brownfield deployments, where Cisco Unified CM and Cisco Prime Collaboration Provisioning are already LDAP-integrated separately, set the flag as "Synchronization and Authentication". • For Greenfield deployments, we recommend you to set the flag as "None". If you select this option, Cisco Unified CM need not synchronize with AD to authenticate users. When a new user is created in Cisco Prime Collaboration Provisioning, and if Cisco Unified CM is set to Authenticate Only with LDAP, then the user account is pushed into Cisco Unified CM and the user is marked as an LDAP synchronized user in Cisco Unified CM. This functionality ensures that Cisco Unified CM contains only users that have services assigned to them. • Synchronization—Select this option if you have enabled LDAP synchronization alone in Unified Communications Manager. • Synchronization and Authentication—Select this option if you have enabled LDAP synchronization and authentication in Unified Communications Manager. The value you choose must exactly match the value configured in Cisco Unified Communications Manager. If Cisco Unified Communications Manager is integrated with an external LDAP, users are not

Field	Description
	created through Provisioning; instead they are synchronized through Cisco Unified Communications Manager. While provisioning a service, if a user is not available on Cisco Unified Communications Manager, the workflow subsystem waits for a predefined period of time (24 hours by default) for the user to be available on Cisco Unified Communications Manager and then continues provisioning the service. The 24-hour period can be configured on Provisioning in the ipt.properties file. Change the following settings: • dfc.oem.extdir.retries: 24 • dfc.oem.extdir.retry_interval: 3600 **Note** To modify the ipt.properties file, contact Cisco TAC. **Note** You must restart Cisco Prime Collaboration Provisioning if you make any changes to ipt.properties file. **Note** LDAP integration is available only for Cisco Unified Communications Manager versions 5.0 and later. For details on single LDAP synchronization, refer the note below this table.
Extension Mobility Details (Optional)	
Service Name	The name of the Extension Mobility Service configured on a Call Processor.
Service URL	The URL of the Extension Mobility Service configured on the Call Processor: http://<ip-address>/ emapp/EMAppServlet?device=#DEVICENAME# Where ip-address is the name or the IP address of the server where Extension Mobility is installed. **Note** The Service Name and Service URL you enter in Cisco Prime Collaboration Provisioning should match the Service Name and Service URL in Cisco Unified Communications Manager.

Note **Single LDAP Synchronization**

Cisco Prime Collaboration Provisioning 10.5.1 and above versions along with Cisco Unified CM 10.5.1 and above versions support a feature called single LDAP synchronization, which eliminates the need to have different LDAP synchronization policies.

During single LDAP synchronization, Cisco Prime Collaboration Provisioning alone is LDAP integrated. Cisco Unified CM is configured with LDAP Directory and authentication information. Cisco Prime Collaboration Provisioning synchronizes users from LDAP. And when the user information is pushed into Cisco Unified CM, Cisco Prime Collaboration Provisioning marks appropriate flags through which Cisco Unified CM identifies the user as LDAP synchronized user. **Remember:**

- This feature is supported only with Cisco Unified CM and not with other UC applications like Cisco Unity Connection and Cisco IM & Presence.
- This feature is supported only with Cisco Prime Collaboration Provisioning10.5.1 and above, when used with Cisco Unified CM 10.5.1 and above.
- LDAP Directory information in Cisco Prime Collaboration Provisioning and Cisco Unified CM should match. Any out-of-band changes in Cisco Unified CM require Cisco Unified CM user synchronization.

For Greenfield deployments: Cisco Prime Collaboration Provisioning takes care of pushing the required LDAP configurations into Cisco Unified CM. The LDAP integration flag is set to "None".

For Brownfield deployments: Where Cisco Unified CM is already LDAP integrated and users are synchronized into Cisco Unified CM, you are recommended to use the existing LDAP policies in Cisco Prime Collaboration Provisioning and Cisco Unified CM as is. The LDAP integration flag is set to "Synchronization & Authentication".

Table 2: Unified Message Processor Fields

Field	Description
Voicemail Pilot Number This option is available only in the Getting Started Wizard.	Directory number dialed to access voicemail messages.

Field	Description
LDAP Integration **Note** This option is available only for Cisco Unity Connection.	Specifies whether Cisco Unity Connection is integrated with an external LDAP. If you select Yes, while provisioning voicemail account, Cisco Prime Collaboration Provisioning searches the LDAP users list in Cisco Unity Connection. If the user name is available in the list, it imports the user details and provision a voicemail account. If you select No, Cisco Prime Collaboration Provisioning does not search the LDAP users list and follows the normal process for provisioning voicemail account. **Note** It is always recommended to run LDAP synchronization in Unity Connection before performing LDAP synchronization in Cisco Prime Collaboration Provisioning.
Username	This field is case-sensitive. The username supplied in this field should match the following: • Cisco Unity Connection—Any user with Cisco Unity Connection administrator privileges. • Cisco Unity Express—Username of the router where Cisco Unity Express is installed.
Password	This field is case-sensitive. The password supplied in this field should match the following: • Cisco Unity Connection—Administrator password. • Cisco Unity Express—Password for the router where Cisco Unity Express is installed.

OS Administrator Name
Note This option is available only for Cisco Unity Connection 10.0 and above.
	The OS administrator name is created during the installation of Cisco Unity Connection.
	When the default administrator credentials are changed, you should create a new proxy user in Unity Connection.
	To create a proxy user, login as administrator in Cisco Unity Connection and enter the following CLI commands:
	`utils cuc proxy usrcreate`
	`utils cuc proxy usrpasswd`
	`utils cuc proxy enable`

Field	Description
OS Administrator Password **Note** This option is available only for Cisco Unity Connection 10.0 and above.	The OS administrator password is created during the installation of Cisco Unity Connection.
Enable Password	Enable password for the router where Cisco Unity Express is installed.
Create by Import	Indicates whether a new account should be created on an Exchange server for new voicemail accounts created in Cisco Unity. If selected, creating user accounts on the Exchange server is prevented. User accounts are associated only if they already exist on the Exchange server.
(Optional) Line User Name	Username for the Cisco Unity Express module.
Line User Password	Password for the Cisco Unity Express module.
Service Engine Interface Number	The interface number of the Cisco Unity Express service engine on the router.

Table 3: LDAP and ACS Server Configuration Fields

Field	Description
LDAP Server Type	Type of LDAP server. The types are: • Microsoft Active Directory • Microsoft ADAM or Lightweight Directory Services • AD 2012 • Sun One • Oracle Directory Server • OpenLDAP For information about the Microsoft AD versions supported by Cisco Prime Collaboration Provisioning, see Supported Devices for Prime Collaboration Provisioning.
Server Port	Port number for the AAA server. Default Non-Secure port: 389 Default Secure port: 636

Field	Description
Backup Server Port	Port number for the backup AAA server.
Backup Server IP Address	IP address of the backup server.
Admin Distinguished Name	The administrative user ID of the LDAP manager that has access rights to the LDAP directory. For example, a user, John Doe, with userID = jdoe must enter John Doe. **Note** If admin is a user in windows domain Cisco, just enter admin (username with domain prefix such as cisco\admin does not work).
Admin Password	The administrative users password (LDAP manager).

Field	Description
LDAP User Search Base	

Field	Description
	This should be the search base of the Admin user account entered in "Admin Distinguished Name". This is used for connection tests. **Note** Domain LDAP Synchronization and User LDAP Authentication uses the search base defined in domains for synchronization and authentication. LDAP server searches for users under this base. You must enter the CN or OU details when you enter the search base. Just dc=cisco, dc=com do not work; you must also specify the CN or OU part. For example, cn=users, dc=eta, dc=com. If you have configured two different user groups, for example, • OU=Organization, OU=Accounts, DC=aaa, DC=com • OU=Service, OU=Accounts, DC=aaa, DC=com The search base to be entered is OU=Accounts, DC=aaa, DC=com. If a user in OU=Organization user group is configured as Admin DN, then all the users in Organization user group can login to Prime Collaboration, but the users in Services user group cannot login. Similarly, if a user in OU=Services user group is configured as Admin DN, then all the users in Services user group can login to Prime Collaboration, but not the users in Organization user group. If you configure a user in top level as Admin DN, then all the users under that level can log into Prime Collaboration. For example, if a user in OU=Accounts user group is configured as Admin DN, then all the users in Organization and Services user groups can login to Prime Collaboration. **Note** • LDAP authentication fails if you enter special characters in the search base. • OU is for Oracle, and CN is for Windows LDAP Example: • For Windows LDAP Server: Admin Distinguished

Field	Description
	Name-CN=administrator, CN=Users, DC=pcp, DC=cisco, DC=com LDAP User Search Base--CN=Users, DC=pcp, DC=cisco, DC=com • For Oracle Server: Admin Distinguished Name-OU=Oracle, OU=Users, DC=pcp, DC=cisco, DC=com LDAP User Search Base--OU=Users, DC=pcp, DC=cisco, DC=com
Use SSL	You should check this check box if Cisco Prime Collaboration Provisioning should use Secure Socket Layer (SSL) encryption for the transmission channel between Cisco Prime Collaboration Provisioning and the AAA server.
ACS Authentication Protocol	Protocol used by the ACS server for authentication.
Enable Data Encryption	Enables data encryption between Cisco Prime Collaboration Provisioning and the ACS server.

Working with Cisco Unity Connection Device

Cross-launching Serviceability from Infrastructure Setup

For Cisco Unity Connection clustering and failover support, be aware of the following:

- When adding a Cisco Unity Connection that includes a Cisco Unity Connection cluster server pair, add the publisher and Subscriber server of the pair.

If a network has more than one location, individually add all of the locations for either the Cisco Unity Connection server or Cisco Unity Connection cluster to Cisco Prime Collaboration Provisioning.

If Cisco Unity is used in the configuration, configure the Cisco Unified Communications Manager voicemail ports.

For more information on these devices, see Setting Up Devices for Prime Collaboration Provisioning.

Cisco Prime Collaboration Provisioning allows an administrator to cross launch Cisco Unity Connection Serviceability and Cisco Unified Serviceability from the configured Cisco Unity Connection and Cisco Unified Communications Manager respectively.

Note Cross launching serviceability is supported for Cisco Unified Communications Manager and Cisco Unity Connection devices only.

When you cross-launch serviceability, you can access the serviceability UI and perform any operation directly on the server of that device. To learn about serviceability in Cisco Unified Communications Manager, see theCisco Unified Serviceability Administration Guide. Similarly, to learn about serviceability in Cisco Unity Connection, see Administration Guide for Cisco Unity Connection Serviceability for details.

With the cross-launching serviceability feature, Cisco Prime Collaboration Provisioning facilitates you to activate, deactivate, start and stop services (directly) on all managed nodes. Rest your mouse pointer over Cisco Unified Communications Manager or Cisco Unity Connection in the device table, and click the quick view icon to view the **Serviceability** cross launch link under the Actions pane.

Adding Cisco TelePresence Management Suite

You can enable scheduling for video endpoints by adding a Cisco TelePresence Management Suite (TMS) device that synchronizes with Cisco Unified Communications Manager to discover devices. Note that the scheduling is executed only in Cisco TMS and you can launch the scheduling UI from Prime Collaboration Provisioning.

Step 1 Add Cisco TMS (see the procedure on Adding Devices).

Step 2 Associate an application user to Cisco TMS. For each Cisco Unified Communications Manager that you want to provision, you can select the application user to be associated with Cisco TMS. Choose **Device Setup. Hover over Quick View and Click UC Services tab**. Under **TMS Service**, select an application user for a Cisco Unified Communications Manager, and click **Apply**.

Note that the application user must belong to these groups: Standard CCM Admin Users and Standard CTI Enabled and have one of the following roles:

Standard AXL API Access, Standard CCM Admin Users, Standard CTI Enabled, Standard CUReporting, Standard RealtimeAndTraceCollection, Standard SERVICEABILITY

Step 3 Provision an endpoint. See Provisioning Services for Users.To enable scheduling: In the **Service Specific Configuration Layout**, click **Enable Scheduling**.

The endpoint is added and provisioned on the Cisco Unified Communications Manager for an application user that is associated to the specific Service Area.

Note When you create a new order for an endpoint, you could have many services pointing to different Cisco Unified Communications Managers. In this case, you must select the Service Areas applicable for the respective Cisco Unified Communications Manager (under Unified Communication Services).

Deleting Devices

To completely remove a device from Cisco Prime Collaboration Provisioning, you must delete it through the Infrastructure Setup page. Note the following points when you are deleting a device:

- No active released orders, including unrecoverable or recoverable errors.
- No active batch projects.
- No synchronizations in progress.

  If these conditions are not met, a message appears on the page when you attempt to delete a device. Avoid performing any activities until the deletion is complete.

- Before deleting a AAA server, ensure that it is not assigned to a Domain.
- There must not be any pending orders on the device.
- Before deleting a device, ensure that you perform a domain synchronization to avoid any stale entries into the system.

To delete devices:

Step 1 Put Cisco Prime Collaboration Provisioning in maintenance mode. (See Maintenance Mode.)

Step 2 Choose **Device Setup**.

Step 3 In the Device Setup page, select the device you want to delete and click **Delete**.

Step 4 In the confirmation dialog box, click **OK** to confirm deletion.

Enabling Cisco Jabber Services

You can enable Cisco Jabber services for devices in Cisco Prime Collaboration Provisioning. Cisco Jabber services allow you to interact with instant messaging and presence.

From 10.6, with the Administrator privileges, you can select up to four Cisco Jabber types:

- Cisco Jabber for Desktop
- Cisco Jabber for Android
- Cisco Jabber for iPhone
- Cisco Jabber for Tablet

Note Cisco Jabber service is available for Cisco Unified Communications Manager 9.1.1 and above version, and Cisco Unified Presence only.

To enable Cisco Jabber service for a call processor:

Step 1 Choose **Device Setup**.

Step 2 Hover over Quick View of the device and click the UC Services tab and click **Enable**

Step 3 Enter the SIP Profile, Service Profile, Softkey template fields and Service Parameter information, and click Apply. See Infrastructure Data Object Fields for information on these fields. You can click View Order to see the order details in the User Record page. The date when the Jabber Service is enabled is displayed.

Note Once you enable Cisco Jabber service for a call processor, you cannot edit or disable it.

Configuring Conference Now Service

You can enable, disable or edit Conference Now services for devices. By enabling Conference Now service, you can setup an IVR (Interactive Voice Response) guided conference calls from your device. You can enable Conference Now service using batch provisioning or quick UI.

After enabling the Conference Now service, you can provision this service to the user in the User Service Ordering page. To enable this service to the user see,Table 1.

The user can modify the Conference Now end-user settings in the self-care UI, only if Conference Now service is enabled for the user. For more details see, Table 1.

Note Conference Now service is available only for Cisco Unified CM 11.x and later versions.

You must have minimum one media resource group list and calling search space configured in the Unified Communications Manager to enable Conference Now service.

To enable or edit Conference Now service:

Step 1 Choose **Device Setup**.

Step 2 Mouse over the information icon against the desired device name. The **Device Details** quick view appears.

Step 3 In the **Device Details** quick view, click the **UC Services** tab.

Step 4 Click **Enable/Edit** against the Conference Now service.

Note The **Edit** button appears, when the conference now service is enabled for the device.

The **Enable** button will be dimmed if there are no media resource group list or calling search space configured in the Unified Communications Manager.

Step 5 Enter the required details in the **Conference Now Service** page and click **Apply**. For details about these fields, see Table 4: Conference Now service fields. An asterisk next to a field indicates a mandatory field.

Note To disable Conference Now service, click **Disable**.

Table 4: Conference Now service fields

Field	Description
Conference Now IVR Directory Number	Enter a DID (Direct Inward Dial) number for a Cisco Unified Communication Manager cluster so that external callers can access this number
Description	Enter the description.
Route Partition	Select an existing route partition or create a new route partition as required. • To Select an existing route partition, click **Use Existing** radio button, and choose an existing partition from the drop-down list. • To create a new route partition, click **New** radio button, and enter the route partition name in the text box. Route partition is used to restrict access to the Conference Now number or pattern
Maximum Wait Time For Host	Choose the time in minutes for the participants to wait for the host to join the conference. This field specifies the maximum wait time for an attendee before a host joins the meeting. If the host has not yet joined the meeting. After the timer expires, the attendee is disconnected automatically.
MOH Source While Participant is Waiting	Choose an MOH (Music On Hold) source to be played, while the participant is waiting for the host to join the conference. If nothing is selected, the default Network Hold MOH/MOH Source configured on the service parameter is used.
Media Resource Group List	Choose the media resource group list to associate with IVR (Interactive Voice Response) Media Resource.
Calling Search Spaces	Choose a calling search space to add to the selected route partition.

Troubleshooting

Issue : Conference Now Service button is dimmed.

Recommended Action

Check whether the required objects (Media Resource List and Calling Search Space) are configured in Cisco Unified CM.

- If the objects are configured in Cisco Unified CM, perform infrastructure synchronization.
- If the objects are not configured in Cisco Unified CM, add them via batch provisioning or infrastructure configuration UI.

Configuring Emergency Location Service

Emergency location service is used to determine the caller's location when an emergency call is placed. It is designed for very small customer environments of about 100 emergency numbers.

The following infrastructure object must be configured to use Emergency Location Service. You can configure these objects using batch provisioning or quick UI.

- Route Pattern.
- Translation Pattern.
- Device Pool.
- Emergency Location (ELIN) Group.

You can view the details of the Emergency Location (ELIN) group associated with the device pool defined in respective service area in the Service Area report page. You can also view the status of Emergency Location (ELIN) Service associated with the service area in the service area quick view, while ordering service for the user.

Note Emergency Location service settings are applicable only if the emergency location support is enabled in the Cisco Unified Communications Manager.

You must have minimum one route pattern and translation pattern configured in the Unified Communications Manager to enable Emergency Location service.

Emergency Location service is available only for Cisco Unified CM 11.x and later versions.

You can enable, disable or edit the existing settings of Emergency Location service in Cisco Prime Collaboration Provisioning.

To enable or edit Emergency Location service:

Step 1 Choose **Device Setup**.

Step 2 Mouse over the information icon against the desired device. The **Device Details** quick view appears.

Step 3 In the **Device Details** quick view, click the **UC Services** tab.

Step 4 Click **Enable/Edit** against the Emergency Location service.

Note The **Edit** button appears, when the Emergency Location service is enabled for the device.

The **Enable** button will be grayed out if no route pattern or translation pattern is configured in the Unified Communications Manager.

Step 5 In the Emergency Location service page add ELIN group. To add ELIN group, see Adding ELIN Groups.

Select the required **Route Patterns** and **Translation Patterns**. For details about these fields, see Table 5: Emergency Location service fields, on page 19.

Note To disable Emergency Location Service, click **Disable**. Disabling emergency location service results in the following changes in Unified Communications Manager : ELIN groups will be deleted, device pools will be disassociated from the ELIN groups, and ELIN settings in translation and route patterns will be disabled. These changes are updated in Cisco Prime Collaboration Provisioning after the subsequent infrastructure synchronization or change notification.

Troubleshooting

- **Issue :** Emergency Location Service button greyed out

  Recommended Action :

  Check whether the required objects (Translation Pattern and Route Pattern) are configured in Cisco Unified CM.

  - If the objects are configured in Cisco Unified CM, perform infrastructure synchronization.
  - If the objects are not configured in Cisco Unified CM, add them via batch provisioning or infrastructure configuration UI.

- **Issue :**Emergency Location Service is enabled in the device, but Service Area quick view shows Emergency Location is disabled.

  Recommended Action : Enable Emergency Location on the Device Pool associated with the Service Area using batch provisioning.

Adding ELIN Groups

ELIN group is a collection of ELIN numbers, each group should have as many ELINs created as are needed to support simultaneous emergency calls. For example, to support five simultaneous calls five ELINs would be needed in an ELIN group.

To add ELIN groups :

Step 1 Click **ADD** in the emergency location service page.

Step 2 Enter the ELIN group name, ELIN number and select the partition. You can add or remove ELIN number and partition by clicking the + or - button. Select the required device pool to associate with the ELIN group.

Step 3 Click **Save**.

Note To update the ELIN group details, select the required ELIN group and click **Edit** .

Table 5: Emergency Location service fields

Field	Description
ELIN group name	Enter a unique name for the emergency location group. ELIN group name can only contain alphanumeric characters (a-z, A-Z, 0-9), period (.), space, underscore (_) and hyphen (-).

ELIN number	Enter unique DID numbers registered in the Public Safety Answering Point (PSAP).
Partition	Select the partition that contains the numbers used by the PSAP to call into the network.
Device Pool	Select the device pools to which the ELIN group must be associated. You can associate ELIN group to multiple device pool. You can also associate ELIN group to the device pool in Device Pool Infrastructure Configuration Product Fields. For details, see Device Pool Infrastructure Configuration Product Fields.
Route Pattern	Select the route pattern that can route emergency calls to the local public safety answering point (PSAP). You can configure the route pattern to route the emergency call by checking **Is an Emergency Services Number** checkbox in Route Pattern Infrastructure Configuration Product Fields. For details see, Route Pattern Infrastructure Configuration Product Fields.
Translation Pattern	Select translation pattern that can manipulate and identify the dialed digits as emergency service number before it routes a call. You can configure the translation pattern to identify the emergency call numbers by checking **Is an Emergency Services Number** checkbox in Translation Pattern Infrastructure Configuration Product Fields. For details see, Translation Pattern Infrastructure Configuration Product Fields.