Provision Unified CM for Unified CCX

When you access Unified CCX Administration for the first time in a cluster, the system automatically initiates the cluster setup procedure once for each cluster to perform the following tasks:

- Identify Unified CCX license files
- Enter information about Unified CM Administrative XML Layer (AXL) and Unified CM Telephony and RmCm providers

You can modify the Unified CM information from Unified CCX. See the *Cisco Unified Contact Center Express Install and Upgrade Guide* for detailed information on how to perform the initial system setup using the Unified CCX Administration web interface.

The following topics explain how to modify the Unified CM information from Unified CCX:

- Configure Unified Communications Manager Information, on page 1
- Unified Communications Manager for Unified CCX Configuration, on page 6

Configure Unified Communications Manager Information

During initial setup of Unified CCX using the Unified CCX Administration web interface, the administrator who installed the Unified CCX should have already provided the Unified Communications Manager IP address and hostname(s). Upload the Cisco Unified Communications Manager Tomcat certificate from Cisco Unified Communications Manager (CUCM) into the Unified CCX Tomcat trust store using the Cisco Unified OS Administration interface. The administrator must also provide the Administrative XML Layer (AXL) authentication (user ID and password) information.

The Unified Communications Manager Configuration web page allows you to configure and update the AXL authentication information, Unified Communications Manager Telephony subsystem information, and RmCm Provider configuration information from within Unified CCX.

This page has three blocks of information: AXL service details, Unified Communications Manager Telephony Provider details, and RmCm Provider details.

If the same user ID (Application User in CUCM) is used as CUCM admin and is also configured as AXL user in Unified CCX, the user ID may get locked if wrong password is used multiple times to login to CUCM. If the user ID gets locked, you will not be able send AXL requests such as, Create Call Control groups, Triggers, and so on from Unified CCX to CUCM. The best practice is to create AXL specific admin credentials.

Note Before regenerating CUCM certificates, disable **SRTP** in **System Parameters Configuration** page of Unified CCX Administration.

For any modification related to CUCM certificates, see *Administration Guide for Cisco Unified Communications Manager*. After completing all the modifications related to CUCM certificates, enable **SRTP** in Unified CCX Administration.

Modify AXL Information

To change previously configured AXL information, complete the following steps.

Note If you want to change the credentials, change first in Unified Communications Manager and then in Unified CCX. Otherwise, Unified CCX might have issues communicating with Unified Communications Manager.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **System** > **Cisco Unified CM Configuration**.

The Cisco Unified Communications Manager Configuration web page opens.

Step 2 Go to the **AXL Service Provider Configuration** section to modify the AXL information using the following fields:

Field	Description
AXL Service Provider Configuration	
Selected AXL Service Providers	Lists the AXL service providers that are configured. You can have a maximum of two AXL service providers in the list. Select one or both the AXL service providers and click the right arrow to remove them from the selected list. The removed AXL Service Providers are moved to the available list for future use. Arrange the order of the selected entries using the up and down arrows.
Available AXL Service Providers	Lists the AXL service providers that are available in the Unified CM cluster. Select one or two AXL service providers and click the Left arrow to add them to the selected list. **Note** Make sure you configure multiple AXL providers running the AXL Service for a redundant system.
Cluster Wide Parameters	

Field	Description
User Name	The Unified Communications Manager User ID. This information is provided during cluster setup in the Unified CCX installation process. When you select an AXL Service Provider, the corresponding username is automatically displayed in this field. This is a mandatory field.
Password	Password for the Unified Communications Manager User ID. This information is provided during cluster setup in the Unified CCX installation process. When you select an AXL Service Provider, the corresponding user password is automatically displayed in this field. This is a mandatory field.

Step 3 After logging in to the Unified CCX Administration web interface, follow these steps to update the AXL password:

a) Log in to Unified Communications Manager Administration web interface and update the password for the application user (AXL provider).

b) Navigate back to **System** > **Cisco Unified CM Configuration** web page of Unified CCX and enter the new password in the Password field.

A dialog box prompts you to confirm the AXL username and password. Reenter the AXL user ID and password and click **Login**.

The system validates the data and takes you back to the Unified Communications Manager configuration page.

c) Enter the updated password once again to validate and click **Update**.

The AXL password is updated successfully and you should be able to log in to Unified CCX Administration web interface of Unified CCX with the new AXL password.

Step 4 Click **Update** at the top of the Cisco Unified Communications Manager Configuration web page or the **Update** button that displays at the bottom of the web page to save the changes. The Unified Communications Manager Configuration web page refreshes to display the new settings.

The selected AXL services are now enabled. If the selected AXL services cannot be enabled, an error message instructs you to reselect AXL service providers.

Modify Unified Communications Manager Telephony Information

Note The Unified Communications Manager Telephony client is installed in the background after you configure the Unified Communications Manager Telephony user. The Unified Communications Manager Telephony client runs in the background and verifies that the right version and the right client are installed.

Configuring the Unified Communications Manager Telephony user does not automatically install the Unified Communications Manager Telephony client. This is normally done during activation of Unified CCX Engine in component activation (see *Cisco Unified Contact Center Express Serviceability Administration Guide*). To install it manually, go to **Subsystems** > **Unified CM Telephony** and select the **Cisco JTAPI Resync** submenu option from the Unified CCX Administration menu bar.

The updated list of CTI Managers within a cluster are listed in this section. If for any reason the Unified Communications Manager is not functioning or if the Unified CCX cannot connect to the Unified Communications Manager, information that is obtained from the most recent connection is saved as part of the bootstrap information.

To change previously configured Unified Communications Manager Telephony information, complete the following steps.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **System** > **Unified CM Configuration**.

The Cisco Unified Communications Manager Configuration web page opens.

Step 2 Scroll down to the **Unified CM Telephony Subsystem - Unified CM Telephony Provider Configuration** section and reconfigure the Unified Communications Manager Telephony information using the following fields.

Field	Description
Unified CM Telephony Subsystem—Unified CM Telephony Provider Configuration	
Selected CTI Managers	Lists the CTI Managers that are configured. You can have a maximum of two CTI Managers in the list. Select one or both the CTI Managers and click the right arrow to remove them from the selected list. The removed CTI Managers are moved to the available list for future use. Arrange the order of the selected entries using the up and down arrows. **Note** SRTP settings remain unchanged, even if the **Selected CTI Managers** are changed.
Available CTI Managers	Lists the CTI Managers that are available in the Unified CM cluster. Select one or two CTI Managers and click the Left arrow to add them to the selected list.
Cluster Wide Parameters	
User Prefix	The syntax of the User ID is: <*userprefix*>_<*nodeid*> For example, if you set this field to **cti_user**, the User ID for Node 1 will be **cti_user_1**. This is a mandatory field.
Password	Password that you defined for the User ID in Unified Communications Manager. If a CTI Manager is already selected, the corresponding password is displayed in this field. This is a mandatory field.

Field	Description
Confirm Password	Reenter the password that you provided in the Password field. This is a mandatory field.

Step 3 Click **Update** at the top of the Cisco Unified Communications Manager Configuration web page or click the **Update** button that displays at the bottom of the web page to save the changes.

The Unified Communications Manager Configuration web page refreshes to display the new settings.

The newly selected CTI Manager is now enabled. If the selected CTI Manager cannot be enabled, an error message instructs you to reselect CTI Managers.

Note In a HA over WAN deployment of Unified CCX, the JTAPI user will be created only for the selected node. To create JTAPI user for the HA node, you have to explicitly select the HA node, make necessary updates, and click **Update**.

Modify RmCm Provider Information

The list of all CTI Managers available in a cluster are saved as part of the bootstrap information. You can select any available CTI Managers listed in the Available CTI Managers list box in this page.

Note The RmCm Provider specified through the Unified CCX Administration is automatically created in Unified Communications Manager. You do not need to use the Unified Communications Manager web interface to create the user.

To change previously configured RmCm provider information or to configure a new RmCm Provider, complete the following steps.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **System** > **Unified CM Configuration**.

The Unified Communications Manager Configuration web page opens.

Step 2 Scroll down to **RmCm Subsystem - RmCm Provider Configuration** and reconfigure the selected CTI Manager using the following fields:

Field	Description
RmCm Subsystems—RmCm Provider Configuration	
Selected CTI Managers	Lists the CTI Managers that are configured. You can have a maximum of two CTI Managers in the list. Select one or both the CTI Managers and click the right arrow to remove them from the selected list. The removed CTI Managers are moved to the available list for future use. Arrange the order of the selected entries using the up and down arrows.

Field	Description
Available CTI Managers	Lists the CTI Managers that are available in the Unified CM cluster. Select one or two CTI Managers and click the Left arrow to add them to the selected list.
User ID	User prefix for the Unified Communications Manager User IDs to be created in Unified Communications Manager. **Note** The RmCm User Id must neither be a standard user created on Cisco Unified CM by default nor be a part of Standard CM Super Users group. If a CTI Manager is already selected, the corresponding user name is displayed in this field. If you change the CTI Managers, be sure to enter the corresponding user prefix for the selected service. This is a mandatory field.
Password	Password you defined for the User ID in Unified Communications Manager. If a CTI Manager is already selected, the corresponding password is displayed in this field. If you change the CTI Manager, be sure to enter the corresponding password for the selected service. This is a mandatory field.
Confirm Password	Reenter the password that you provided in the Password field. This is a mandatory field.

Step 3 Click **Update** at the top of the Cisco Unified Communications Manager Configuration web page or click the **Update** button that displays at the bottom of the web page to save the changes.

The Unified Communications Manager Configuration web page refreshes to display the new settings.

The newly selected RmCm Provider is now enabled. If the selected RmCm Provider cannot be enabled, an error message instructs you to reselect RmCm Provider.

Unified Communications Manager for Unified CCX Configuration

To enable Unified CCX to communicate with Unified Communications Manager, you also need to assign extensions for the users who will be agents in your Unified CCX system.

Note If you delete a Unified CCX user with Administrative rights from Unified Communications Manager, you can still log in to the Unified CCX Administration web interface as an application user.

Note Q Signaling (QSIG) and Path Replacement (PR) features of Unified Communications Manager are not supported by Unified CCX.

Invoke Unified Communications Manager Administration

Begin the process of configuring Unified Communications Manager by connecting to the Unified Communications Manager Administration web interface.

To connect to the Unified Communications Manager Administration web interface, complete the following steps.

Procedure

Step 1 From a web browser on any computer on your network, enter the following URL: **https://***servername***/ccmadmin**.

In this example, *servername* is the hostname or IP address of your Unified Communications Manager server.

A Security Alert dialog box is displayed.

Step 2 Click the appropriate button.

Step 3 At the main Cisco Unified Communications Manager Administration web page, enter the Unified Communications Manager username and password, and then click **Login**.

The Unified Communications Manager Administration web page appears.

You are now ready to use the Unified Communications Manager Administration web interface to configure users for Unified CCX.

Unified Communications Manager Users as Unified CCX Agents

Warning Do not configure Unified Communications Manager users having the same username/password as the application administration credentials (configured during installation). Doing so may restrict the Unified Communications Manager when shared across multiple Unified CCX servers.

Note When there is a change in the configuration data on the Unified Communications Manager, the team configuration is lost on the Unified CCX. You must reconfigure the teams in the Unified CCX or restore data from DRS.

Agent ID

When logging in to the desktop, agents use the Unified Communications Manager user ID and password. Unified Communications Manager limits agent IDs to 128 alphanumeric characters, but Unified CCX limits the agent IDs to 64 alphanumeric characters. For more information about Agent ID configuration, see the Agent Configuration section.

Attention Unified Communications Manager user ID should not exceed 64 alpha-numeric characters. If user ID exceeds 64 alphanumeric characters, Unified CCX does not synchronize users from Unified Communications Manager.

Agent Name

Agent name includes the first name and last name. The following is the limit for agent name in Unified CCX:

- English-based script (German, Spanish, English, and so on)—50 characters
- Non-English script (Arabic, Chinese, Cyrillic, and so on)—16 characters

Attention If the agent name exceeds the limit, Unified CCX truncates the name to 50 or 16 characters respectively and stores.

RmCm uses the Unified Communications Manager database to determine which devices it can control and provides an interface method for getting the Media Access Control (MAC) address of the calling party.

After you install RmCm, you get access to the Unified Communications Manager database. The database stores parameters that initialize Unified Communications Manager Telephony, user profiles, application logic, network-specific configuration information, and Directory Number Associations such as Primary Extension and Unified CCX Extension.

The Primary Extension field represents the primary directory number for the end user. End users can have multiple lines on their phones. From the drop-down list box, choose a primary extension when associating devices for this end user.

Unified CCX Extension allows you to define Unified Communications Manager users as Unified CCX agents in Unified Communications Manager.

To assign Unified CCX devices to end users and application users in the Unified Communications Manager, these users must first exist in Unified Communications Manager. If these users do not exist, you must first add the users. See the *Cisco Unified Communications Manager Administration Guide* to obtain detailed information about the Unified CCX web interface and configuration procedures. After adding the end user and the application user, be sure to modify their Unified CCX settings.

Agents and Supervisors with IDs That Match Reserved Words Cannot Sign In

Do not use the following reserved words for agent ID or supervisor ID because these IDs conflict with system account names that are used internally within the Unified CCX server:

System\Components	Reserved words
Unified CCX Web Chat	admin

System\Components	Reserved words
Cisco Finesse	admin
	finesse
	fippa
	xmpprootowner
	presencelistener

Note

- If a user tries to sign in with a reserved word for the agent ID or supervisor ID, the sign-in fails.
- Do not use the reserved words for IDs whether they are upper case, lower-case, or any combination of both cases. For example, admin, ADMIN, or Admin.

Guidelines for Agent Phone Configuration

Follow these guidelines when configuring agent phones for Unified CCX agents:

- Choose **Device** > **Phone** in Unified Communications Manager Administration. The Find and List Phones window is displayed.

  Enter search criteria to locate a specific phone and click **Find**. A list of phones that match the search criteria is displayed. Click the device name of the phone to which you want to add a directory number. The Phone Configuration window is displayed.

  In the Unified Communications Manager Administration Phone Configuration web page, select the required Association Information (on the left) to get to the Directory Number Configuration web page. On this page, make the following changes:

  - In the Multiple Call/Call Waiting Settings section, set the Maximum Number of Calls to 2 (default is 4) for Cisco Unified IP Phones 7900 Series and 3 for Cisco Unified IP Phones 8961, 9951, and 9971.

Note If you are using Cisco Finesse for your agent desktop, you must set the Maximum Number of Calls to 2 for all agent phones.

  - In the Multiple Call/Call Waiting Settings section, set the Busy Trigger value to 1 (default is 2).
  - In the Call Forward and Call Pickup Settings section, verify that you do not forward any Unified Communications Manager device to the Unified CCX extension of an agent.
  - In the Call Forward and Call Pickup Settings section, verify that you do not configure the Unified CCX extension of an agent to forward to a Unified CCX route point.

- Secure Real-Time Transport Protocol (SRTP) based recording is now supported. You can disable Secure Real-Time Transport Protocol (SRTP) when configuring a Cisco Unified Communications product. You can disable SRTP for a specified device or for the entire Unified Communications Manager:

- For a specified device—Choose **Device** > **Phone**. In the Find and List Phone page, select the required phone device. In the Phone Configuration page for the selected phone, scroll down to the Protocol Specific Information section. To turn off SRTP on the phone device, select any one of the **Non Secure SCCP Profile auth by** choices from the drop-down list in **SCCP Phone Security Profile** or **SCCP Device Security Profile** field.
- For the entire Unified Communications Manager cluster—Choose **System** > **Enterprise Parameters**. In the Enterprise Parameters Configuration page, scroll down to the Securities Parameters section, to verify that the corresponding value for the Cluster Security Mode field is 0. This parameter indicates the security mode of the cluster. A value of 0 indicates that phones will register in nonsecure mode (no security).

- The Unified CCX extension for the agent must be listed within the top 4 extensions on the device profile. Listing the extension from position 5 on will cause Unified CCX to fail to monitor the device, so the agent will not be able to log in.
- Do not forward any Unified Communications Manager device to the Unified CCX extension of an agent.
- Do not configure the Unified CCX extension of an agent to forward to a Unified CCX route point.
- Do not use characters other than the numerals 0 to 9 in the Unified CCX extension of an agent.
- Do not configure two lines on an agent phone with the same extension when both lines exist in different partitions.
- Do not assign a Unified CCX extension to multiple devices.
- Do not configure the same Unified CCX extension in more than one device or device profile. (Configuring a Unified CCX extension in one device or device profile is supported.)
- To use Cisco Unified IP Phones 9900 Series, 8900 Series, and 6900 Series as agent devices, the RmCm application user in Unified Communications Manager needs to have “Allow device with connected transfer/conference” option assigned to itself.

To determine a list of Unified CCX agent devices supported by Cisco Finesse Desktop, see the Unified CCX Compatibility related information, located at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Modify Existing Unified Communications Manager Users

To use any version of Unified Communications Manager, you must first ensure that you define Unified Communications Manager users as Unified CCX agents in Unified Communications Manager. After you perform this task, these Unified CCX agents can be combined into Resource Groups, assigned Skills, and placed in CSQs.

Note In Unified CCX, this operation is called “associating a device.”

Note Be sure to assign Unified CCX devices to both end users and application users in the Unified Communications Manager web interface.

To assign devices to an end user, you must access the End User Configuration window for that user. The End User Configuration window in Unified Communications Manager Administration allows the administrator to add, search, display, and maintain information about Unified Communications Manager end users.

To assign devices to an application user, you must access the Application User Configuration window for that user. The Application User Configuration window in Unified Communications Manager Administration allows the administrator to add, search, display, and maintain information about Unified Communications Manager application users.

Note If Enterprise Mobility (EM) is used together with both Cisco Unified Communications Manager release 8.0 or later and Cisco Unified Communications Manager, the Resource Manager application user must be associated with the device profile and not with the device.

To modify the Unified CCX Extension settings for existing Unified Communications Manager users who are Unified CCX agents, complete the following steps:

Note If you change or update an end user ID in Unified Communications Manager, Unified CCX resets the end user's resource name, skills, and team to default values.

Procedure

Step 1 Connect to the Unified Communications Manager Administration web interface.

The Unified Communications Manager Administration web page appears.

Step 2 Choose **User Management** > **End User**.

The Find and List End Users page displays. Use the two drop-down list to search for an end user.

Tip To find all end users that are registered in the database, click **Find** without entering any search text. A list of discovered end users is displayed. Then, skip to Step 6.

Step 3 From the first Find end user where drop-down list, choose one of the listed criteria.

Step 4 From the second Find end user where drop-down list, choose one of the listed criteria.

Step 5 Specify the appropriate search text, if applicable, and click **Find**.

A list of discovered end users is displayed.

Step 6 From the list of records, click the end user name that matches your search criteria.

The End User Configuration page opens, displaying the configuration information for the end user that you chose.

Step 7 In the Controlled Devices list box below the Device Information section, select the device and click the Down arrow below the Available Profiles list box. If the device that you want to associate with this end user is not displayed in this pane, do the following to associate devices with an end user:

a) From the Device Information pane, click **Device Association**. The User Device Association page opens.

b) Finding a Device: Because you may have several devices in your network, Cisco Unified Communications Manager lets you locate specific devices on the basis of specific criteria. Click **Find**. All or matching records are displayed. You can change the number of items that is displayed in each page by choosing a different value from the Rows per Page drop-down.

c) Associating a Device: From the Device association for (this particular end user) pane, choose the devices that you want to associate with this end user by checking the box to the left of the device names. You can also use the buttons at the bottom of the window to select and deselect devices to associate with the end user.

d) To complete the association, click **Save Selected/Changes**.

e) From Related Links drop-down list in the upper right corner of the web page, choose **Back to User**, and click **Go**.

The End User Configuration page is displayed, and the associated devices that you chose are displayed in the Controlled Devices pane.

Step 8 Select the required device and save your changes to associate that device with this end user.

After the device is associated, the Controlled Devices field displays the description information (for example, the MAC address) that the end user controls.

Step 9 In the End User Configuration page, scroll down to the **Directory Number Associations** section.

Step 10 In the **Primary Extension** field drop-down list and the **IPCC Extension** field drop-down list, choose the required agent extension for this device.

These fields represent the primary directory number for the end user. End users can have multiple lines on their phones. If you have a single line, be sure to select the same extension for both fields.

Step 11 Click **Update** to apply the changes.

The specific End User Information page for this user appears, with the message that the update was successful.

Step 12 From the Unified Communications Manager Administration menu bar, choose **User Management** > **Application User**. RmCm Providers are referred to as application users in Unified Communications Manager.

Note When you associate one device with the Unified CCX agent (end user), you must also be sure to associate the same device with the Unified CCX RmCm Provider (application user).

The Find and List Application Users window is displayed. Use the two drop-down list to search for the application users in Unified Communications Manager.

Tip To find all application users registered in the database, click **Find** without entering any search text. A list of discovered end users is displayed. Then, skip to Step 16.

Step 13 From the first Find application user where drop-down list, choose one of the listed criteria.

Step 14 From the second Find application user where drop-down list, choose one of the listed criteria,

Step 15 Specify the appropriate search text, if applicable, and click **Find**.

A list of discovered application users is displayed.

Step 16 From the list of records, click the application user name that matches your search criteria.

The window displays the application user that you choose.

Step 17 Repeat Step 7 and Step 8 for the selected Application User.

These steps ensure that the Unified Communications Manager application users are also defined as Unified CCX agents in Unified Communications Manager.

Step 18 Click **Update** to apply the changes.

The specific Application Information page for this user appears, with the message that the update was successful.

See the "User Management Configuration" section in the *Cisco Unified Communications Manager Administration Guide* for detailed information on how to configure an end user and application user using Unified Communications Manager.

Now that you have defined the agent in Unified Communications Manager, you can configure agents in Unified CCX. Before you configure the agent, you will also need to configure resource groups and CSQs.

Assign Unified Communications Manager Users as Cisco TelePresence Virtual Agents

The Cisco TelePresence application enables enterprises to create a live, face-to-face interaction with customers over the network. This solution allows rapid deployment of a virtual contact center infrastructure. Agents using Cisco TelePresence are referred to as virtual agents in this guide. Virtual agents connect to callers using Unified CCX, which incorporates ACD, CTI, and Unified IP IVR with Cisco Unified Communications Manager and providing the entire solution on one server.

Note For more information on the Cisco TelePresence solution, see https://www.cisco.com/en/US/products/ps7060/index.html.

The following guidelines apply for the Cisco TelePresence integration with Unified CCX:

- The only commonly supported codec for Unified CCX and Cisco TelePresence is G711.
- The following supervisor features are not supported:
  - Monitoring and Recording is not supported for Cisco TelePresence integration with Unified CCX.

Follow this procedure to assign Unified Communications Manager users as virtual agents:

Procedure

Step 1 Identify the required Cisco TelePresence system that will participate as a virtual agent in the Unified CCX application.

a) Note the Unified Communications Manager extension of the Cisco TelePresence deployment.

Note The Cisco Unified IP Phone 7970G and Cisco TelePresence system must be assigned the same extension in Unified Communications Manager, because they both share the same line.

b) Note the MAC address or the Directory Number of the Cisco Unified IP Phone 7970G connected to the identified Cisco TelePresence system.

Tip From the Unified CCX perspective, this is another SIP endpoint.

Step 2 Associate the Cisco Unified IP Phone 7970G with the Unified Communications Manager user to configure this user as a virtual agent.

Step 3 Associate the Cisco Unified IP Phone 7970G with the RmCm provider.

Note Do not associate the corresponding Cisco TelePresence system with the RmCm provider.

Configure Tool for Auto-Registered Phones Support (TAPS)

The Tool for Auto-Registered Phone Support (TAPS) loads a preconfigured phone setting on a phone. The TAPS works in conjunction with the Bulk Administration Tool (BAT). After the BAT is used to bulk add phones with dummy MAC addresses to Cisco Unified Communications Manager Administration, you can plug the phones into the network.

The administrator or users can then dial a TAPS directory number that causes the phone to download its configuration. At the same time, the phone gets updated in the Unified Communications Manager database with the correct MAC address of the phone. Refer to Configuring the Bulk Administration Tool (BAT) if you are not familiar with the BAT.

For the TAPS to function, you must make sure that Auto-registration is enabled in Cisco Unified Communications Manager Administration (select **System** > **Cisco Unified CM**). Follow the instructions in the procedure below to install and configure TAPS application with Unified CCX.

Procedure

Step 1 Log in to Cisco Unified Communications Manager Administration and choose **Application** > **Plugins** from the Cisco Unified Communications Manager Administration menu bar.

Step 2 In the Find and List Plugins web page, search for "Cisco TAPS" and click **Find**.

Step 3 Download the TAPS_AAR.aar file to your client PC, which is used for accessing Unified Communications Manager Administration and Unified CCX Administration.

Step 4 Install Unified CCX. See the *Cisco Unified Contact Center Express Install and Upgrade Guide*, available at https://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Step 5 After installing Unified CCX, follow these steps from the User Configuration page in Unified CCX Administration:

a) In the Cisco Unified Communications Manager Users list, select the Cisco Unified Communications Manager user whom you want to designate as the Cisco Unified CCX administrator and who can configure TAPS.

b) Click the **left arrow** (<) to move the selected user to the Cisco Unified CCX Administrator list.

c) Click **Finish**. The Cisco Unified CCX Setup Result Information window is displayed. This window confirms the result of the initial setup. The Cisco Unified CCX engine will restart.

d) Close your web browser.

Step 6 Log in to Cisco Unified CCX Administration as the Unified CCX application administrator, who can configure TAPS. After installing and configuring Unified CCX and Unified Communications Manager, follow this procedure to set up TAPS:

a) From the Unified CCX Administration menu bar, choose **Applications** > **AAR Management**. Click **Browse** and upload the TAPS_AAR.aar file that you downloaded in Step 3 from Unified Communications Manager.

On successful upload, you will see a confirmation message in the status bar at the top of the AAR Management web page.

Note For TAPS configuration, you need to restart the Unified CCX engine and Unified CCX Cluster View Daemon (CVD). You can restart the CVD using the CLI command,

utils service service name stop/start.

b) After restarting the CVD, log in once again to Cisco Unified CCX Administration as the Unified CCX application administrator. From the Unified CCX Administration menu bar, choose **Subsystems** > **Unified CM Telephony** > **Call Control Group**. Click **Add New** and provide the Call Control Group Configuration values for TAPS using the following fields:

- Group ID
- Number of CTI Ports
- Media Termination Support
- Device Name Prefix
- Starting Directory Number

c) From the Unified CCX Administration menu bar, choose **Subsystems** > **Cisco Unified CM Telephony** > **Triggers**. Click **Add New** and specify values for the following mandatory fields:

- Directory Number
- Language
- Application Name
- Device Name
- Description
- Call Control Group:

  The call control group types can be Inbound or Outbound for Unified CCX running with Unified Communications Manager.

d) Choose **Subsystems** > **Cisco Unified CM Telephony** > **Data Resync** from the Cisco Unified CCX Administration menu bar to check and resynchronize the JTAPI data between Cisco Unified Communications Manager and Cisco Unified CCX.
e) From the Unified CCX Administration menu bar, choose **Applications** > **Application Management**. The Application Management web page opens, displaying the details of existing applications.
f) Click the **Add New** icon or button. The Add a New Application web page opens.
g) From the Application Type drop-down menu, choose Cisco Script Application and click **Next**. The Cisco Script Application configuration web page opens.
h) In the Script field, select the script "/TAPS.aef" from the drop-down list and enter the IP address of the Cisco Unified Communications Manager in the text box below the Script drop-down list.
i) Check the check box against **Cisco_Unified_CM_IP_Address** field.
j) Click the **Yes** radio button in the Enabled field.
k) Click **Update**.

l) Log in to Cisco Unified Communications Manager Serviceability Page and restart the TAPS Service.