Cisco Unified Communications Manager

Cisco Unified Communications Manager Interaction

Cisco Unified Communications Manager is an open, industry-standard call processing system. Cisco Unified Communications Manager software sets up and tears down calls between phones, integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages the components of the telephony system, such as the phones, the access gateways, and the resources necessary for features such as call conferencing and route planning. Cisco Unified Communications Manager also provides:

- Firmware for phones
- Certificate Trust List (CTL) and Identity Trust List (ITL) files using the TFTP and HTTP services
- Phone registration
- Call preservation, so that a media session continues if signaling is lost between the primary Communications Manager and a phone

For information about configuring Cisco Unified Communications Manager to work with the phones described in this chapter, see the documentation for your particular Cisco Unified Communications Manager release.

Note If the phone model that you want to configure does not appear in the Phone Type drop-down list in Cisco Unified Communications Manager Administration, install the latest device package for your version of Cisco Unified Communications Manager from Cisco.com.

Phone Addition Methods

After installation, you can choose one of the following options to add phones to the Cisco Unified Communications Manager database.

- Add phones individually with Cisco Unified Communications Manager Administration
- Add multiple phones with the Bulk Administration Tool (BAT)
- Autoregistration
- BAT and the Tool for Auto-Registered Phones Support (TAPS)

Before you add phones individually or with BAT, you need the MAC address of the phone.

For more information about the Bulk Administration Tool, see the documentation for your particular Cisco Unified Communications Manager release.

If your Cisco Unified Communications Manager is set up to automatically register new phones, you can get new phones working quickly. You need to set up the phone to connect to your Cisco Unified Communications Manager. The new phones are assigned DNs and profiles based on the phone type.

To support autoregistration, you need to set up profiles for the phone models or use the standard profiles.

For more information on autoregistration, see the Cisco Unified Communications Manager documentation.

Manually Add a Phone to Cisco Unified Communications Manager

You can manually configure the your phone in Cisco Unified Communications Manager (Unified CM) so the phone can register. Some tasks in this procedure are optional, depending on your system and user needs.

For more information on any of the steps, see the documentation for your particular Unified CM release.

Perform the configuration steps in the following procedure using Unified CM Administration.

Before you begin

Before you begin, collect the phone model and the Media Access Control (MAC) address. This information is on the bottom of the phone and on the shipping box label.

From your records, gather the following information:

- Physical location of the phone
- Name or user ID of the phone user
- Device pool
- Partition, calling search space, and location information
- Directory number (DN) to assign to the phone
- Phone usage information that affects the phone button template, phone features, services, or applications

Verify that you have sufficient unit licenses for your phone. For more information, see the licensing document for your particular (Unified CM) release.

Procedure

Step 1 Define the Device Pools. Select **System** > **Device Pool**.

Device Pools define common characteristics for devices, such as a region, date or time group, and phone button template.

Step 2 Define the Common Phone Profile. Select **Device** > **Device settings** > **Common Phone Profile**.

Common phone profiles provide data that the Cisco TFTP server requires, and common phone settings, such as Do Not Disturb and feature control options.

Step 3 Define a Calling Search Space. In Unified CM Administration, click **Call Routing** > **Class of Control** > **Calling Search Space**.

A Calling Search Space is a collection of partitions that are searched to determine how a dialed number is routed. The calling search space for the device and the calling search space for the directory number are used together. The directory number CSS takes precedence over the device CSS.

Step 4 Configure a security profile for the device type and protocol. Select **System** > **Security** > **Phone Security Profile**.

Step 5 Set up the phone. Select **Device** > **Phone**.

a) Locate the phone you want to modify, or add a new phone.

b) Configure the phone by completing the required fields in the Device Information pane of the **Phone Configuration** window.

- MAC Address (required): Make sure that the value comprises 12 hexadecimal characters.
- Description: Enter a useful description to help you when you search information about this user.
- Device Pool (required)
- Common Phone Profile
- Calling Search Space
- Location
- Owner (User or Anonymous), and if User is selected, the Owner User ID

The device with its default settings is added to the Unified CM database.

For information about Product Specific Configuration fields, see the **?** Button Help in the Phone Configuration window.

Note If you want to add both the phone and user to the Unified CM at the same time, see the documentation for your particular Unified CM release.

c) In the Protocol Specific Information area of this window, choose a Device Security Profile and set the security mode.

Note Choose a security profile based on the overall security strategy of the company. If the phone does not support security, choose a nonsecure profile.

d) In the Extension Information area, check the Enable Extension Mobility check box if this phone supports Cisco Extension Mobility.
e) Click **Save**.

Step 6 Select **Device** > **Device Settings** > **SIP Profile** to set up SIP parameters.

Step 7 Select **Device** > **Phone** to configure directory numbers (lines) on the phone by completing the required fields in the Directory Number Configuration window.

a) Find the phone.
b) In the Phone Configuration window, click **Line 1** on the left pane of the window.

Conference phones have only one line.

c) In the Directory Number field, enter a valid number that can be dialed.

Note This field should contain the same number that appears in the Telephone Number field in the End User Configuration window.

d) From the Route Partition drop-down list, choose the partition to which the directory number belongs. If you do not want to restrict access to the directory number, choose **<None>** for the partition.
e) From the Calling Search Space drop-down list, choose the appropriate calling search space. The value that you choose applies to all devices that are using this directory number.
f) In the Call Forward and Call Pickup Settings area, choose the items (for example, Forward All, Forward Busy Internal) and corresponding destinations to which calls should be sent.
g) In the Line 1 on Device pane, configure the following fields:

- Display (Internal Caller ID field): You can enter the first name and last name of the user of this device so that this name displays for all internal calls. Leave this field blank to have the system display the phone extension.
- External Phone Number Mask: Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line. You can enter a maximum of 24 numeric and "X" characters. The Xs represent the directory number and must appear at the end of the pattern.

Example:

If you specify a mask of 408902XXXX, an external call from extension 6640 displays a caller ID number of 4089026640.

This setting applies only to the current device unless you check the check box at the right (Update Shared Device Settings) and click **Propagate Selected**. The check box at the right displays only if other devices share this directory number.

h) Select **Save**.

For more information about directory numbers, see the documentation for your particular Cisco Unified Communications Manager release.

Step 8 (Optional) Associate the user with a phone. Click **Associate End Users** at the bottom of the Phone Configuration window to associate a user to the line that is being configured.

a) Use **Find** in conjunction with the Search fields to locate the user.
b) Check the box next to the user name, and click **Add Selected**.

The user name and user ID appear in the Users Associated With Line pane of the Directory Number Configuration window.

c) Select **Save**.

The user is now associated with Line 1 on the phone.

Step 9 (Optional) Associate the user with the device:

a) Choose **User Management** > **End User**.
b) Use the search boxes and **Find** to locate the user you have added.
c) Click on the user ID.
d) In the Directory Number Associations area of the screen, set the Primary Extension from the drop-down list.
e) (Optional) In the Mobility Information area, check the Enable Mobility box.
f) In the Permissions Information area, use the **Add to Access Control Group** buttons to add this user to any user groups.

For example, you may want to add the user to a group that is defined as a Standard CCM End User Group.

g) To view the details of a group, select the group and click **View Details**.
h) In the Extension Mobility area, check the Enable Extension Mobility Cross Cluster box if the user can use for Extension Mobility Cross Cluster service.
i) In the Device Information area, click **Device Associations**.
j) Use the Search fields and **Find** to locate the device that you want to associate to the user.
k) Select the device, and click **Save Selected/Changes**.
l) Click **Go** next to the "Back to User" Related link in the upper right corner of the screen.
m) Select **Save**.

Step 10 Configure the phone services and assign them. Select **Device** > **Device Settings** > **Phone Services**.

Step 11 (Optional) Associate a user with a user group. Select **User Management** > **User Settings** > **Access Control Group**.

Assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access for system users.

Phone Feature Configuration

You can set up phones to have a variety of features, based on the needs of your users. You can apply features to all phones, a group of phones, or to individual phones.

When you set up features, the Cisco Unified Communications Manager Administration window displays information that is applicable to all phones and information that is applicable to the phone model. The information that is specific to the phone model is in the Product Specific Configuration Layout area of the window.

For information on the fields applicable to all phone models, see the Cisco Unified Communications Manager documentation.

When you set a field, the window that you set the field in is important because there is a precedence to the windows. The precedence order is:

1. Individual phones (highest precedence)
2. Group of phones
3. All phones (lowest precedence)

Set Up Phone Features for All Phones

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration as an administrator.
Step 2 Select **System** > **Enterprise Phone Configuration**.
Step 3 Set the fields you want to change.
Step 4 Check the **Override Enterprise Settings** check box for any changed fields.
Step 5 Click **Save**.
Step 6 Click **Apply Config**.
Step 7 Restart the phones.

Note This will impact all phones in your organization.

Set Up Phone Features for a Group of Phones

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration as an administrator.
Step 2 Select **Device** > **Device Settings** > **Common Phone Profile**.
Step 3 Locate the profile.
Step 4 Navigate to the Product Specific Configuration Layout pane and set the fields.
Step 5 Check the **Override Enterprise Settings** check box for any changed fields.
Step 6 Click **Save**.
Step 7 Click **Apply Config**.
Step 8 Restart the phones.

Set Up Phone Features for a Single Phone

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration as an administrator.
Step 2 Select **Device** > **Phone**
Step 3 Locate the phone associated with the user.
Step 4 Navigate to the Product Specific Configuration Layout pane and set the fields.
Step 5 Check the **Override Common Settings** check box for any changed fields.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

Step 8 Restart the phone.

Product Specific Configuration

The following table describes the fields in the Product Specific Configuration Layout pane on Cisco Unified Communications Manager (Unified CM). Some fields in this table only display in the **Device** > **Phone** page.

Table 1: Product Specific Configuration Fields

Field Name	Field Type Or Choices	Default	Description
Cisco Discovery Protocol (CDP): Switch Port	Disabled Enabled	Enabled	Controls Cisco Discovery Protocol on the phone.
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port	Disabled Enabled	Enabled	Enables LLDP-MED on the LAN port.
LLDP Asset ID	String, up to 32 characters		Identifies the asset ID that is assigned to the phone for inventory management.
LLDP Power Priority	Unknown Low High Critical	Unknown	Assigns a phone power priority to the switch, thus enabling the switch to appropriately provide power to the phones.
Customer support upload URL	String, up to 256 characters		Provides the URL for the Problem Report Tool (PRT).
Webex Activation Code	String, up to 256 characters		Activates the Webex cloud account from Unified CM instead of from the device. This field is only for Unified CM Calling with Control Hub
Proxy Settings for Webex	URL		The proxy server and port to access Webex cloud. This field is only for Unified CM Calling with Control Hub

Phone Configuration Files

Configuration files for a phone are stored on the TFTP server and define parameters for connecting to Cisco Unified Communications Manager. In general, any time you make a change in Cisco Unified Communications Manager that requires the phone to be reset, a change is automatically made to the phone configuration file.

Configuration files also contain information about which image load the phone should be running. If this image load differs from the one currently loaded on a phone, the phone contacts the TFTP server to request the required load files.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For more information, see the documentation for your particular Cisco Unified Communications Manager release. A phone requests a configuration file whenever it resets and registers with Cisco Unified Communications Manager.

A phone accesses a default configuration file named XmlDefault.cnf.xml from the TFTP server when the following conditions exist:

- You have enabled autoregistration in Cisco Unified Communications Manager
- The phone has not been added to the Cisco Unified Communications Manager database
- The phone is registering for the first time

Device Security Overview

Security features keep your phone network secure and prevent someone from tampering with the Cisco Unified Communications Manager (Unified CM) server, your data, or the call-signaling and media-stream.

Your device supports the following security features:

- Signed firmware images, secure start-up process, and secure provisioning with signed configuration files.
- Certificate Trust Lists (CTL) and Initial Trust Lists (ITL).
- Locally Significant Certificates (LSC) and Cisco issued Manufacturing Installed Certificates (MIC).
- SIP call security features including call and media encryption.

You verify a successful MIC installation from the **Status messages** screen of the **Settings** menu on the phone. Verify the CTL and ITL installation from the device log files.

For additional information about security, see *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Certificates Overview

A certificate is a file that contains the certificate holder name, public key and digital signature for the authority that issues it. It proves the identity of the certificate owner.

Cisco Unified Communications Manager (Unified Communications Manager) uses certificates that include the public-key infrastructure (PKI) in order to validate server and client identity, and to enable encryption. When another system tries to connect to Unified Communications Manager it presents the certificate to verify its identity. Cisco Unified Communications Manager doesn't trust the other system, and will deny access unless it has a matching certificate in the appropriate trust store.

Your device supports two types of X.509 certificates:

- Manufacturer Installed Certificate (MIC)—Cisco IP devices are pre-installed with the MIC and you can't delete or modify it. The Certificate Authority (CA) certificates CAP-RTP-001, CAP-RTP-002, Cisco_Manufacturing_CA and Cisco Manufacturing CA SHA2 are pre-installed in the Cisco network administration server to trust the MIC. A MIC can’t be used once the validity is expired as the MIC CA can't be re-generated.

  You can download a CA certificate from https://www.cisco.com/security/pki/certs/cmca.cer.

- Locally Significant Certificate (LSC)—The LSC includes the public key for the Cisco IP device, which is signed by the Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF) private key. It's not installed on the device by default. Administrators have full control over LSC. A CAPF CA Certificate can be regenerated and a new LSC can be issued to the devices whenever required.

  The LSC is generated from your Unified Communications Manager. For more information, see *Security Guide for Cisco Unified Communications Manager*.

When deploying a new device, a **Device Security Profile** must be configured. The Certificate Authority Proxy Function (CAPF) must be operational in order to use a LSC with a security profile. The MIC can be utilized with a security profile as well.

The default device security profile is **Standard SIP Non-Secure Profile**, which doesn't use encryption.

802.1X Authentication

Your Cisco IP Phone supports 802.1X Authentication with a Locally Significant Certificate (LSC) or a Manufacturing Installed Certificate (MIC).

If you deploy for Cisco Unified Communications Manager (Unified CM) Calling or for Unified CM Calling with Control Hub, then you can use both LSCs and MICs. But only a MIC is used for Webex Calling with Control Hub.

Both EAP-TLS and EAP-FAST are supported for authentication.

Cisco IP Phones and Cisco Catalyst switches traditionally use Cisco Discovery Protocol (CDP) to identify each other and determine parameters such as VLAN allocation and inline power requirements. CDP does not identify locally attached workstations.

Support for 802.1X authentication requires several components:

- Cisco IP Phone: The phone initiates the request to access the network. The phone contains an 802.1X supplicant, which allows network administrators to control the connectivity of IP phones to the LAN switch ports.
- Cisco Identity Services Engine (ISE), or other third-party authentication server: Configure the server with the Certificate Authority (CA) for the MIC or LSC.
- Cisco Catalyst Switch or other third-party switch: The switch must support 802.1X, so it can act as the authenticator and pass the messages between the phone and the authentication server. After the exchange completes, the switch grants or denies the phone access to the network.

You must perform the following actions to configure 802.1X:

- Configure the other components before you enable 802.1X Authentication on the phone.
- Configure Voice VLAN: Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.

  Enabled: If you are using a switch that supports multidomain authentication, you can continue to use the voice VLAN.

  Disabled: If the switch does not support multidomain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN.

Enable 802.1X Authentication on Your Device

Enable 802.1X Authentication if you want to control access to your network.

Procedure

Step 1 Tap the top-left corner of the phone screen.
Step 2 Tap **Settings** from the list of menu options.
Step 3 Scroll down and tap **Network connection**.
Step 4 Tap **Open Ethernet settings**.
Step 5 Toggle Use IEEE 802.1X to **On**.
Step 6 Reboot the phone after you configure your setting.