



Cisco IP Conference Phone Installation

- [Verify the Network Setup, on page 1](#)
- [Activation Code Onboarding for On-premises Phones, on page 2](#)
- [Activation Code Onboarding and Mobile and Remote Access, on page 3](#)
- [Enable Autoregistration for Phones, on page 3](#)
- [Install the Conference Phone \(7832\), on page 5](#)
- [Set Up the Phone from the Setup Menus, on page 6](#)
- [Configure the Network Settings, on page 8](#)
- [Verify the Phone Startup, on page 12](#)
- [Change a User's Phone Model, on page 12](#)

Verify the Network Setup

As they deploy a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service. For information and a checklist for setting up and configuring a Cisco IP telephony network, see the documentation for your particular Cisco Unified Communications Manager release.

For the phone to operate successfully as an endpoint in your network, your network must meet specific requirements. One requirement is the appropriate bandwidth. The phones require more bandwidth than the recommended 32 kbps when they register to Cisco Unified Communications Manager. Consider this higher bandwidth requirement when you configure your QoS bandwidth. For more information, refer to *Cisco Collaboration System 12.x Solution Reference Network Designs (SRND)* or later (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html).



Note The phone displays the date and time from Cisco Unified Communications Manager. The time displayed on the phone can differ from the Cisco Unified Communications Manager time by up to 10 seconds.

Procedure

Step 1 Configure a VoIP Network to meet the following requirements:

- VoIP is configured on your routers and gateways.

- Cisco Unified Communications Manager is installed in your network and is configured to handle call processing.

Step 2 Set up the network to support one of the following:

- DHCP support
- Manual assignment of IP address, gateway, and subnet mask

Related Topics

[Cisco Unified Communications Manager Documentation](#)

Activation Code Onboarding for On-premises Phones

You can use Activation Code Onboarding to quickly set up new phones without autoregistration. With this approach, you control the phone onboarding process using the one of the following:

- Cisco Unified Communications Bulk Administration Tool (BAT)
- Cisco Unified Communications Manager Administration interface
- Administrative XML Web Service (AXL)

Enable this feature from the **Device Information** section of the Phone Configuration page. Select **Require Activation Code for Onboarding** if you want this feature to apply to a single on-premises phone.

Users must enter an activation code before their phones can register. Activation Code Onboarding can be applied to individual phones, a group of phones, or across an entire network.

This is an easy way for users to onboard their phones because they only enter a 16-digit activation code. Codes are entered either manually or with a QR code if a phone has a video camera. We recommend that you use a secure method to give users this information. But if a user is assigned to a phone, then this information is available on the Self Care Portal. The audit log records when a user accesses the code from the portal.

Activation codes can only be used once, and they expire after 1 week by default. If a code expires, you will have to provide the user with a new one.

You will find this approach an easy way to keep your network secure because a phone cannot register until the Manufacturing Installed Certificate (MIC) and activation code are verified. This method is also a convenient way to bulk onboard phones because it doesn't use the Tool for Auto-registered Phone Support (TAPS) or autoregistration. The rate of onboarding is one phone per second or about 3600 phones per hour. Phones can be added with the Cisco Unified Communications Manager Administrative, with Administrative XML Web Service (AXL), or with BAT.

Existing phones reset after they are configured for Activation Code Onboarding. They don't register until the activation code is entered and the phone MIC is verified. Inform current users that you are moving towards Activation Code Onboarding before you implement it.

For more information, see *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 12.0(1)* or later.

Activation Code Onboarding and Mobile and Remote Access

You can use Activation Code Onboarding with Mobile and Remote Access when deploying Cisco IP phones for remote users. This feature is a secure way to deploy off-premises phones when autoregistration is not required. But you can configure a phone for autoregistration when on-premises, and activation codes when off-premises. This feature is similar to Activation Code Onboarding for on-premises phones, but it makes activation code available for off-premises phones also.

Activation Code Onboarding for Mobile and Remote Access requires Cisco Unified Communications Manager 12.5(1)SU1 or later, and Cisco Expressway X12.5 or later. Smart Licensing should be enabled also.

You enable this feature from the Cisco Unified Communications Manager Administration, but note the following:

- Enable this feature from the **Device Information** section of the Phone Configuration page.
- Select **Require Activation Code for Onboarding** if you want this feature to apply just to a single on-premises phone.
- Select **Allow Activation Code via MRA** and **Require Activation Code for Onboarding** if you want to use Activation Onboarding for a single off-premises phone. If the phone is on-premises, it changes to Mobile and Remote Access mode and uses the Expressway. If the phone cannot reach the Expressway, it does not register until it is off premises.

For more information, see the following documents:

- *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 12.0(1)*
- *Mobile and Remote Access Through Cisco Expressway* for Cisco Expressway X12.5 or later

Enable Autoregistration for Phones

The Cisco IP Phone requires Cisco Unified Communications Manager to handle call processing. See the documentation for your particular Cisco Unified Communications Manager release or the context-sensitive help in the Cisco Unified Communications Manager Administration to ensure that Cisco Unified Communications Manager is set up properly to manage the phone and to properly route and process calls.

Before you install the Cisco IP Phone, you must choose a method for adding phones to the Cisco Unified Communications Manager database.

By enabling autoregistration before you install the phones, you can:

- Add phones without first gathering MAC addresses from the phones.
- Automatically add a Cisco IP Phone to the Cisco Unified Communications Manager database when you physically connect the phone to your IP telephony network. During autoregistration, Cisco Unified Communications Manager assigns the next available sequential directory number to the phone.
- Quickly enter phones into the Cisco Unified Communications Manager database and modify any settings, such as the directory numbers, from Cisco Unified Communications Manager.

- Move autoregistered phones to new locations and assign them to different device pools without affecting their directory numbers.

Autoregistration is disabled by default. In some cases, you might not want to use autoregistration; for example, if you want to assign a specific directory number to the phone, or if you want to use a secure connection with Cisco Unified Communications Manager. For information about enabling autoregistration, see the documentation for your particular Cisco Unified Communications Manager release. When you configure the cluster for mixed mode through the Cisco CTL client, autoregistration is automatically disabled, however you can enable it. When you configure the cluster for nonsecure mode through the Cisco CTL client, autoregistration is not enabled automatically.

You can add phones with autoregistration and TAPS, the Tool for AutoRegistered Phones Support, without first gathering MAC addresses from phones.

TAPS works with the Bulk Administration Tool (BAT) to update a batch of phones that were already added to the Cisco Unified Communications Manager database with dummy MAC addresses. Use TAPS to update MAC addresses and to download predefined configurations for phones.

Cisco recommends that you use autoregistration and TAPS to add fewer than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT).

To implement TAPS, you or the end user dials a TAPS directory number and follows voice prompts. After the process is complete, the phone contains the directory number and other settings, and the phone is updated in Cisco Unified Communications Manager Administration with the correct MAC address.

Verify that autoregistration is enabled and is properly configured in Cisco Unified Communications Manager Administration before you connect any Cisco IP Phone to the network. For information about enabling and configuring autoregistration, see the documentation for your particular Cisco Unified Communications Manager release.

Autoregistration must be enabled in Cisco Unified Communications Manager Administration for TAPS to function.

Procedure

- Step 1** In Cisco Unified Communications Manager Administration, click **System > Cisco Unified CM**.
- Step 2** Click **Find** and select the required server.
- Step 3** In **Auto-registration Information**, configure these fields.
- **Universal Device Template**
 - **Universal Line Template**
 - **Starting Directory Number**
 - **Ending Directory Number**
- Step 4** Uncheck the **Auto-registration Disabled on this Cisco Unified Communications Manager** check box.
- Step 5** Click **Save**.
- Step 6** Click **Apply Config**.
-

Related Topics

[Cisco Unified Communications Manager Documentation](#)

Install the Conference Phone (7832)

After the phone connects to the network, the phone startup process begins, and the phone registers with Cisco Unified Communications Manager. You need to configure the network settings on the phone if you disable the DHCP service.

If you used autoregistration, you need to update the specific configuration information for the phone such as associating the phone with a user, changing the button table, or directory number.

After the phone connects, it determines if a new firmware load should be installed on the phone.

Before you begin

Ensure that you have the latest firmware version installed on your Cisco Unified Communications Manager. Check for updated device packages here:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_00_cucm-device-package-compatibility-matrix.html

Procedure

- Step 1** Choose the power source for the phone:
- Power over Ethernet (PoE)
 - Cisco Unified IP Phone Power Injector
- For more information, see [Ways to Provide Power to Your Conference Phone](#), on page 6.
- Step 2** Connect the phone to the switch.
- If you use PoE, plug the Ethernet cable into the LAN port and plug the other end into the phone.
 - If you use the Cisco Unified IP Phone Power Injector, plug the injector into the LAN port with one Ethernet cable. Connect the power cord to the injector and plug the cord into the electrical outlet. Use another Ethernet cable to connect the injector to the conference phone.
- Each phone ships with one Ethernet cable in the box.
- Step 3** Monitor the phone startup process. This step verifies that the phone is configured properly.
- Step 4** If you do not use autoregistration, manually configure the security settings on the phone.
See [Configure the Security Settings](#).
- Step 5** Allow the phone to upgrade to the current firmware image that is stored on your Cisco Unified Communications Manager.
- Step 6** Make calls with the phone to verify that the phone and features work correctly.
- Step 7** Provide information to end users about how to use their phones and how to configure their phone options. This step ensures that users have adequate information to successfully use their Cisco phones.
-

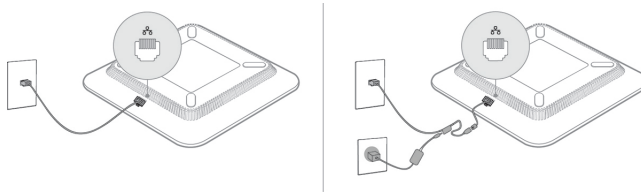
Ways to Provide Power to Your Conference Phone

Your conference phone needs power from one of these sources:

- Power over Ethernet (PoE), which your network supplies.
- Cisco IP Phone Power Injector.
- A PoE Power Cable and Power Cube 3.

The following figure shows the PoE and PoE power cable power options.

Figure 1: Conference Phone Power Options



Set Up the Phone from the Setup Menus

The phone includes many configurable network settings that you may need to modify before the phone is functional for your users. You can access these settings, and change some of them, through menus on the phone.

The phone includes the following setup menus:

- Network Setup: Provides options for viewing and configuring a variety of network settings.
 - IPv4 Setup: This submenu provides additional network options.
 - IPv6 Setup: This submenu provides additional network options.
- Security Setup: Provides options for viewing and configuring a variety of security settings.





Note You can control whether a phone has access to the Settings menu or to options on this menu. Use the **Settings Access** field in the Cisco Unified Communications Manager Administration Phone Configuration window to control access. The **Settings Access** field accepts these values:

- Enabled: Allows access to the Settings menu.
- Disabled: Prevents access to most entries in the Settings menu. The user can still access **Settings > Status**.
- Restricted: Allows access to the User Preferences and Status menu items and allows volume changes to be saved. Prevents access to other options on the Settings menu.

If you cannot access an option on the Admin Settings menu, check the **Settings Access** field.

You configure settings that are display-only on the phone in Cisco Unified Communications Manager Administration.

Procedure

- Step 1** Press **Applications** .
- Step 2** Press **Settings**.
- Step 3** Select **Admin Settings**.
- Step 4** Enter password if required, then click **Sign-In**.
- Step 5** Select **Network Setup** or **Security Setup**.
- Step 6** Perform one of these actions to display the desired menu:
- Use the navigation arrows to select the desired menu and then press **Select**.
 - Use the keypad on the phone to enter the number that corresponds to the menu.
- Step 7** To display a submenu, repeat step 5.
- Step 8** To exit a menu, press **Back** .

Related Topics

- [Restart or Reset the Conference Phone](#)
- [Configure the Network Settings](#), on page 8
- [Configure the Security Settings](#)

Apply a Phone Password

You can apply a password to the phone. If you do, no changes can be made to the administrative options on the phone without password entry on the Admin Settings phone screen.


Procedure

- Step 1** In Cisco Unified Communications Manager Administration, navigate to the Common Phone Profile Configuration window (**Device > Device Settings > Common Phone Profile**).
- Step 2** Enter a password in the Local Phone Unlock Password option.
- Step 3** Apply the password to the common phone profile that the phone uses.
-

Text and Menu Entry From the Phone

When you edit the value of an option setting, follow these guidelines:

- Use the arrows on the navigation pad to highlight the field that you wish to edit. Press **Select** in the navigation pad to activate the field. After the field is activated, you can enter values.
- Use the keys on the keypad to enter numbers and letters.
- To enter letters by using the keypad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the **2** key once for “a,” twice quickly for “b,” and three times quickly for “c.” After you pause, the cursor automatically advances to allow you to enter the next letter.

- Press the softkey  if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press **Revert** before pressing **Apply** to discard any changes that you made.
- To enter a period (for example, in an IP address), press * on the keypad.
- To enter a colon for an IPv6 address, press # on the keypad.



Note The Cisco IP Phone provides several methods to reset or restore option settings, if necessary.

Related Topics

[Restart or Reset the Conference Phone](#)

[Apply a Phone Password](#), on page 7

Configure the Network Settings

Procedure

- Step 1** Press **Settings**.
- Step 2** Select **Admin Settings** > **Network Setup**.
- Step 3** Set the fields as described in [Network Setup Fields, on page 8](#). After you set the fields, you may need to reboot the phone.
-

Network Setup Fields

The Network Setup menu contains fields and submenus for IPv4 and IPv6.

To change some of the fields, you need to turn DHCP off.

Table 1: Network Setup Menu

Entry	Type	Default	Description
IPv4 setup	Menu		See the “IPv4 Setup Submenu” table. This option displays only when the mode or in dual-stack mode.
IPv6 setup	Menu		See the “IPv6 Setup Submenu” table.
Host name	String		Host name of the phone. If using DHCP, this name is automatically assigned.

Entry	Type	Default	Description
Domain name	String		Name of the Domain Name System (DNS) domain in which the phone resides. To change this field, turn off DHCP.
Operational VLAN ID			Operational Virtual Local Area Network (VLAN) that is configured on a Cisco Catalyst switch in which the phone is a member.
Admin VLAN ID			Auxiliary VLAN in which the phone is a member.
SW Port Setup	Auto Negotiate 10 Half 10 Full 100 Half 100 Full	Auto Negotiate	Speed and duplex of the switch port, where: <ul style="list-style-type: none"> • 10 Half = 10-BaseT/half duplex • 10 Full = 10-BaseT/full duplex • 100 Half = 100-BaseT/half duplex • 100 Full = 100-BaseT/full duplex
LLDP-MED: SW Port	Disabled Enabled	Enabled	Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.

Table 2: IPv4 Setup Submenu

Entry	Type	Default	Description
DHCP	Disabled Enabled	Enabled	Enables or disables the use of DHCP.
IP Address			Internet Protocol version 4 (IPv4) address of the phone. To change this field, turn off DHCP.
Subnet Mask			Subnet mask that the phone uses. To change this field, turn off DHCP.
Default Router 1			Default router used that the phone uses. To change this field, turn off DHCP.

Entry	Type	Default	Description
DNS Server 1			<p>Primary Domain Name System (DNS) server (DNS Server 1) that the phone uses.</p> <p>To change this field, turn off DHCP.</p>
Alternate TFTP	No Yes	No	Indicates whether the phone is using an alternative TFTP server.
TFTP Server 1			<p>Primary Trivial File Transfer Protocol (TFTP) server that the phone uses.</p> <p>If you set the Alternate TFTP option to On, you must enter a nonzero value for the TFTP Server 1 option. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock the file before you can save changes to the TFTP Server 1 option. In this case, the phone deletes the file when you save changes to the TFTP Server 1 option. A new CTL or ITL file downloads from the new TFTP Server 1 address.</p> <p>See the TFTP notes after the final table.</p>
TFTP Server 2			<p>Secondary TFTP server that the phone uses.</p> <p>If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock the file before you can save changes to the TFTP Server 2 option. In this case, the phone deletes the file when you save changes to the TFTP Server 2 option. A new CTL or ITL file downloads from the new TFTP Server 2 address.</p> <p>See the TFTP Notes section after the final table.</p>
DHCP Address Released	No Yes	No	

Table 3: IPv6 Setup Submenu

Entry	Type	Default	Description
DHCPv6 Enabled	Disabled Enabled	Enabled	Enables or disables the use of IPv6 DHCP.
IPv6 Address			The IPv6 address of the phone. To change this field, turn off DHCP.
IPv6 Prefix Length			Length of the IPv6 address. To change this field, turn off DHCP.
IPv6 Default Router 1			Default IPv6 router. To change this field, turn off DHCP.
IPv6 DNS Server 1			Primary IPv6 DNS server To change this field, turn off DHCP.
IPv6 Alternate TFTP	No Yes	No	Indicates whether the phone is using an alternative IPv6 TFTP server.
IPv6 TFTP Server 1			Primary IPv6 TFTP server used that the phone uses. See the TFTP Notes section after this table.
IPv6 TFTP Server 2			Secondary IPv6 TFTP server used that the phone uses. See the TFTP Notes section after this table.
IPv6 Address Released	No Yes	No	

Before IPv6 setup options can be configured on your device, IPv6 must be enabled and configured in Cisco Unified Communication Administration. The following device configuration fields apply to IPv6 configuration:

- IP Addressing Mode
- IP Addressing Mode Preference for Signalling

If IPv6 is enabled in the Unified cluster, the default setting for IP addressing mode is IPv4 and IPv6. In this addressing mode, the phone will acquire and use one IPv4 address and one IPv6 address. It can use the IPv4 and the IPv6 address as required for media. The phone uses either the IPv4 or IPv6 address for call control signalling.

For more information about IPv6, see:

- “Common Device Configuration” in *Cisco Unified Communications Manager Feature and Services Guide*, “IPv6 Support in Cisco Unified Communications Devices” chapter.

- *IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.0*, located here:
<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html>

TFTP Notes

When the phone looks for the TFTP server, the phone gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for the TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for the TFTP server in this order:

1. Any manually assigned IPv4 TFTP servers
2. Any manually assigned IPv6 servers
3. DHCP assigned TFTP servers
4. DHCPv6 assigned TFTP servers

For information about the CTL and ITL files, see the *Cisco Unified Communications Manager Security Guide*.

Verify the Phone Startup

After the phone has power connected to it, it automatically cycles through a startup diagnostic process.

Procedure

Power up the phone.

When the main screen displays, it has started up properly.

Change a User's Phone Model

You or your user can change a user's phone model. The change can be required for a number of reasons, for example:

- You have updated your Cisco Unified Communications Manager (Unified CM) to a software version that doesn't support the phone model.
- The user wants a different phone model from their current model.
- The phone requires repair or replacement.

The Unified CM identifies the old phone and uses the old phone's MAC address to identify the old phone configuration. The Unified CM copies the old phone configuration into the entry for the new phone. The new phone then has the same configuration as the old phone.

Limitation: If the old phone has more lines or line buttons than the new phone, the new phone doesn't have the extra lines or line buttons configured.

The phone reboots when the configuration is complete.

Before you begin

Set up your Cisco Unified Communications Manager according to the instructions in the *Feature Configuration Guide for Cisco Unified Communications Manager*.

You need a new, unused phone that comes preinstalled with Firmware Release 12.8(1) or later.

Procedure

- Step 1** Power off the old phone.
 - Step 2** Power on the new phone.
 - Step 3** On the new phone, select **Replace an existing phone**.
 - Step 4** Enter the primary extension of the old phone.
 - Step 5** If the old phone had a PIN assigned, enter the PIN.
 - Step 6** Press **Submit**.
 - Step 7** If there is more than one device for the user, select the device to replace and press **Continue**.
-

