Cisco IP Phone Installation

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**.

Install Cisco IP Phone

After the phone connects to the network, the phone startup process begins, and the phone registers with Cisco Unified Communications Manager. To finish installing the phone, configure the network settings on the phone depending on whether you enable or disable 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.

Note Before using external devices, read External Devices.

For information about installing accessories, see *Cisco IP Phone 7800 and 8800 Series Accessories Guide for Cisco Unified Communications Manager*.

If you only have one LAN cable at your desk, you can plug your phone into the LAN with the SW port and then connect your computer into the PC port. For more information, see Share a Network Connection with Your Phone and Computer, on page 6.

You can also daisy chain two phones together. Connect the PC port of the first phone to the SW port of the second phone.

Caution Do not connect the SW and PC ports into the LAN.

Procedure

Step 1 Choose the power source for the phone:

- Power over Ethernet (PoE)
- External power supply

For more information, see Phone Power Requirements.

Step 2 Connect the handset to the handset port and press the cable into the channel in the phone.

The wideband-capable handset is designed especially for use with a Cisco IP Phone. The handset includes a light strip that indicates incoming calls and waiting voice messages.

Caution Failure to press the cable into the channel in the phone can damage the printed circuit board. The cable channel reduces the strain on the connector and the printed circuit board.

Step 3 Connect a headset or wireless headset. You can add a headset later if you do not connect one now.

Press the cable into the cable channel.

Caution Failure to press the cable into the channel in the phone can damage the printed circuit board inside the phone. The cable channel reduces the strain on the connector and the printed circuit board.

Step 4 Connect a straight-through Ethernet cable from the switch to the network port labeled 10/100/1000 SW on the Cisco IP Phone. Each Cisco IP Phone ships with one Ethernet cable in the box.

Use Category 3, 5, 5e, or 6 cabling for 10 Mbps connections; Category 5, 5e, or 6 for 100Mbps connections; and Category 5e or 6 for 1000 Mbps connections. For more information, see Network and Computer Port Pinouts for guidelines.

Step 5 Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the computer port on the Cisco IP Phone. You can connect another network device later if you do not connect one now.

Use Category 3, 5, 5e, or 6 cabling for 10 Mbps connections; Category 5, 5e, or 6 for 100Mbps connections; and Category 5e or 6 for 1000 Mbps connections. For more information, see Network and Computer Port Pinouts for guidelines.

Step 6 If the phone is on a desk, adjust the footstand. With a wall-mounted phone, you might need to adjust the handset rest to ensure that the receiver cannot slip out of the cradle.

Step 7 Monitor the phone startup process. This step adds primary and secondary directory numbers and features that are associated with directory numbers to the phone, and verifies that the phone is configured properly.

Step 8 If you are configuring the network settings on the phone, you can set up an IP address for the phone by either using DHCP or manually entering an IP address.

See Configure Network Settings, on page 15 and Network Setup.

Step 9 Upgrade the phone to the current firmware image.

Firmware upgrades over the WLAN interface may take longer than upgrading over the wired interface, depending on the quality and bandwidth of the wireless connection. Some upgrades may take more than one hour.

Step 10 Make calls with the Cisco IP Phone to verify that the phone and features work correctly.

See the *Cisco IP Phone 8800 Series User Guide*.

Step 11 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 IP Phones.

Share a Network Connection with Your Phone and Computer

Both your phone and your computer must connect to your network to function. If you only have one Ethernet port, then your devices can share the network connection.

Before you begin

Your administrator must enable the PC port in Cisco Unified Communications Manager before you can use it.

Procedure

Step 1 Connect the phone SW port to the LAN with an Ethernet cable.

Step 2 Connect your computer to the phone PC port with an Ethernet cable.

Set Up Phone from Setup Menus

The Cisco IP Phone includes the following configuration menus:

- Network Setup: Provides options for viewing and configuring network settings such as IPv4-only, IPv6-only, WLAN, and Ethernet.
- Ethernet Setup: The menu items in this submenu provide configuration options to configure the Cisco IP Phone over an ethernet network.
- WiFi Client Setup: The menu items in this submenu provide configuration options to configure the Cisco IP Phone with the wireless local area network (WLAN). Wi-Fi is only supported on Cisco IP Phone 8861 and 8865.

Note The phone PC port is disabled when Wi-Fi is enabled on your phone.

- IPv4 Setup and IPv6 Setup: These submenus of the Ethernet Setup menu and of the WiFi Client Setup menu provide additional network options.
- Security Setup: Provides options for viewing and configuring security settings such as security mode, the trust list and 802.1X authentication.

Before you can change option settings on the Network Setup menu, you must unlock options for editing.

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

- Enabled: Allows access to the Settings menu.
- Disabled: Prevents access to the Settings menu.
- Restricted: Allows access to the User Preferences menu and allows volume changes to be saved. Prevents access to other options on the Settings menu.

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

Procedure

Step 1 Press **Applications** .

Step 2 Select **Admin settings**.

Step 3 Select **Network setup** or **Security setup**.

Step 4 Enter your user ID and password, if required, and click **Sign-In**.

Step 5 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 6 To display a submenu, repeat step 5.

Step 7 To exit a menu, press **Exit** or the back arrow .

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 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, then 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 arrow softkey if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press **Cancel** before pressing **Save** to discard any changes that you made.
- To enter an IP address, you enter values into four segments already divided for you. When you have finished entering the leftmost digits before the first period, use the right arrow key to move to the next segment. The period that follows the leftmost digits is automatically inserted.
- 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

Basic Reset

Apply a Phone Password, on page 8

Enable the Wireless LAN on the Phone

Before you set up a wireless LAN, check to see that your phone supports wireless use. The Cisco IP Phone 8861 and 8865 support a wireless LAN deployment. The Cisco IP Phone 8865NR does not support a wireless LAN.

Ensure that the Wi-Fi coverage in the location where the wireless LAN is deployed is suitable for transmitting voice packets.

If you have enabled the Wi-Fi connectivity for voice and you're using EAP-FAST or PEAP security mode, authenticate the Wi-Fi network with the WLAN Sign in application. WEP, PSK, and open security modes authenticate on the Wi-Fi network.

A fast-secure roaming method is recommended for Wi-Fi users.

Note The phone PC port is disabled when Wi-Fi is enabled on your phone.

For complete configuration information, see the *Cisco IP Phone 8800 Wireless LAN Deployment Guide* at this location:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

The *Cisco IP Phone 8800 Wireless LAN Deployment Guide* includes the following configuration information:

- Wireless network configuration
- Wireless network configuration in Cisco Unified Communications Manager Administration
- Wireless network configuration on the Cisco IP Phone

Before you begin

Make sure that Wi-Fi is enabled on the phone, and the Ethernet cable is disconnected.

Procedure

Step 1 To enable the application, press **Applications**  .

Step 2 Go to **Admin settings** > **Network setup** > **Wi-Fi Client setup** > **Network name**.
You see a list of available wireless access points to which you can connect.

Step 3 Enable the Wireless network.

Set Up the Wireless LAN from Cisco Unified Communications Manager

In Cisco Unified Communications Manager Administration, you must enable a parameter called “Wi-Fi” for the wireless Cisco IP Phone.

Note In the Phone Configuration window in Cisco Unified Communications Manager Administration (**Device** > **Phone**), use the wired-line MAC address when you configure the MAC address. Cisco Unified Communications Manager registration does not use the wireless MAC address.

Perform the following procedure in Cisco Unified Communications Manager Administration.

Procedure

Step 1 To enable the wireless LAN on a specific phone, perform the following steps:

a) Select **Device** > **Phone**.
b) Locate the required phone.
c) Select the **Enabled** setting for the Wi-Fi parameter in the Product Specific Configuration Layout section.
d) Check the **Override Common Settings** check box.

Step 2 To enable wireless LAN for a group of phones,

a) Select **Device** > **Device Settings** > **Common Phone Profile**.
b) Select the **Enabled** setting for the Wi-Fi parameter.

Note To ensure that the configuration in this step works, uncheck the **Override Common Settings** check box mentioned in Step 1d.

c) Check the **Override Common Settings** check box.
d) Associate the phones with that common phone profile using **Device** > **Phone**.

Step 3 To enable wireless LAN for all WLAN-capable phones in your network,

a) Select **System** > **Enterprise Phone Configuration**.
b) Select the **Enabled** setting for the Wi-Fi parameter.

Note To ensure that the configuration in this step works, uncheck the **Override Common Settings** check box mentioned in Step 1d and Step 2c.

c) Check the **Override Common Settings** check box.

Set Up Wireless LAN from Phone

Before the Cisco IP Phone can connect to the WLAN, you must configure the network profile for the phone with the appropriate WLAN settings. You can use the **Network setup** menu on the phone to access the **Wi-Fi client setup** submenu and set up the WLAN configuration.

Note The phone PC port is disabled when Wi-Fi is enabled on your phone.

Note The **Wi-Fi client setup** option does not appear in the **Network setup** menu when Wi-Fi is disabled on the Cisco Unified Communications Manager.

For additional information, see *Cisco IP Phone 8800 Series WLAN Deployment Guide*, located here: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html.

The **User Modifiable** field in the wireless LAN profile controls that ability of the user to configure security modes on the phone. When a user cannot change some of the fields, the fields display in gray.

Before you begin

Configure the wireless LAN from Cisco Unified Communications Manager.

Procedure

Step 1 Press **Applications** .

Step 2 Select **Admin settings** > **Network setup** > **Wi-Fi client setup**.

Step 3 Set up the wireless configuration as described in the following table.

Table 1: WiFi Client Setup Menu Options

Option	Description	To change
Network name	Specifies the Service Set Identifier, a unique identifier for accessing wireless access points. Displays list of available wireless access points.	See Configure Network Settings,
IPv4-only Setup	In the IPv4 Setup configuration submenu, you can do the following: • Enable or disable the phone to use the IP address that the DHCP server assigns. • Manually set the IP Address, Subnet Mask, Default Routers, DNS Server, and Alternate TFTP servers. For more information about the IPv4 address fields, see IPv4 Fields, on page 17.	Scroll to IPv4 Setup and press **Sel**

Option	Description	To change
IPv6-only Setup	In the IPv6 Setup configuration submenu, you can do the following: • Enable or disable the phone to use the IPv6 address that is either assigned by DHCPv6 server or acquired by SLAAC through an IPv6-enabled router. • Manually set the IPv6 Address, Prefix Length, Default Routers, DNS Server, and Alternate TFTP servers. For more information about the IPv6 address fields, see IPv6 Fields, on page 19.	Scroll to IPv6 Setup and press **Select**.
MAC Address	Unique Media Access Control (MAC) address of the phone.	Display only. Cannot configure.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	See Configure Network Settings, on p

Step 4 Press **Save** to make changes or press **Revert** to discard the connection.

Set the Number of WLAN Authentication Attempts

An authentication request is a confirmation of the user's sign-in credentials. It occurs whenever a phone that has already joined a Wi-Fi network tries to reconnect to the Wi-Fi server. Examples include when a Wi-Fi session times out or a Wi-Fi connection is lost and then reacquired.

You can configure the number of times a Wi-Fi phone sends an authentication request to the Wi-Fi server. The default number of attempts is 2, but you can set this parameter from 1 to 3. If a phone fails the authentication, then the user is prompted to sign in again.

You can apply WLAN Authentication Attempts to individual phones, to a pool of phones, or to all the Wi-Fi phones in your network.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Device** > **Phone** and locate the phone.
Step 2 Navigate to the Product Specific Configuration area and set the **WLAN Authentication Attempts** field.
Step 3 Select **Save**.
Step 4 Select **Apply Config**.
Step 5 Restart the phone.

Enable WLAN Prompt Mode

Enable WLAN Profile 1 Prompt Mode if you want a user to sign into the Wi-Fi network when their phone powers-up or resets.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Device** > **Phone**.

Step 2 Locate the phone that you need to set up.

Step 3 Navigate to the Product Specific Configuration area and set the **WLAN Profile 1 Prompt Mode** field to **Enable**.

Step 4 Select **Save**.

Step 5 Select **Apply Config**.

Step 6 Restart the phone.

Set Up a Wi-Fi Profile using Cisco Unified Communications Manager

You can configure a Wi-Fi profile and then assign the profile to the phones that support Wi-Fi. The profile contains the parameters required for phones to connect to the Cisco Unified Communications Manager with Wi-Fi. When you create and use a Wi-Fi profile, you or your users do not need to configure the wireless network for individual phones.

Wi-Fi profiles are supported on Cisco Unified Communications Manager Release 10.5(2) or later. EAP-FAST, PEAP-GTC, and PEAP-MSCHAPv2 are supported in Cisco Unified Communications Manager Release 10.0 and later. EAP-TLS is supported in Cisco Unified Communications Manager Release 11.0 and later.

A Wi-Fi profile enables you to prevent or limit changes to the Wi-Fi configuration on the phone by the user.

We recommend that you use a secure profile with TFTP encryption enabled to protect keys and passwords when you use a Wi-Fi profile.

When you set up the phones to use EAP-FAST, PEAP-MSCHAPv2, or PEAP-GTC authentication, your users need individual user ids and passwords to sign into the phone.

The phones only support one server certificate which can be installed either with SCEP or the manual install method but not both methods. The phones don't support the TFTP method of certificate installation.

Note Phones that use Mobile and Remote Access through Expressway to connect to the Cisco Unified Communications Manager cannot use the Wi-Fi profile. Because you do not have the SSID, authentication mode, and login credentials of the user's phone, you cannot configure a wireless LAN profile for their phone.

Procedure

Step 1 In the Cisco Unified Communications Administration, select **Device** > **Device Settings** > **Wireless LAN Profile**.

Step 2 Click **Add New**.

Step 3 In the **Wireless LAN Profile Information** section, set the parameters:

- **Name**—Enter a unique name for the Wi-Fi profile. This name displays on the phone.
- **Description**—Enter a description for the Wi-Fi profile to help you differentiate this profile from other Wi-Fi profiles.
- **User Modifiable**—Select an option:
  - **Allowed**—Indicates that the user can make changes to the Wi-Fi settings from their phone. This option is selected by default.
  - **Disallowed**—Indicates that the user cannot make any changes to the Wi-Fi settings on their phone.
  - **Restricted**—Indicates that the user can change the Wi-Fi username and password on their phone. But users are not allowed to make changes to other Wi-Fi settings on the phone.

Step 4 In the **Wireless Settings** section, set the parameters:

- **SSID (Network Name)**—Enter the network name available in the user environment to which the phone can be connected. This name is displayed under the available network list on the phone and the phone can connect to this wireless network.
- **Frequency Band**—Available options are Auto, 2.4 GHz, and 5 GHz. This field determines the frequency band that the wireless connection uses. If you select Auto, the phone attempts to use the 5 GHz band first and only uses the 2.4 GHz band when the 5 GHz is not available.

Step 5 In the **Authentications Settings** section, set the **Authentication Method** to one of these authentication methods: EAP-FAST, EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, PSK, WEP, and None.

After you set this field, you may see extra fields that you need to set.

- **User certificate**—Required for EAP-TLS authentication. Select **Manufacturing installed** or **User installed**. The phone requires a certificate to be installed, either automatically from the SCEP or manually from the administration page on the phone.
- **PSK passphrase**—Required for PSK authentication. Enter the 8- 63 character ASCII or 64 HEX character pass phrase.
- **WEP Key**—Required for WEP authentication. Enter the 40/102 or 64/128 ASCII or HEX WEP key.
  - 40/104 ASCII is 5 characters.
  - 64/128 ASCII is 13 characters.
  - 40/104 HEX is 10 characters.
  - 64/128 HEX is 26 characters.
- **Provide Shared Credentials**: Required for EAP-FAST, PEAP-MSCHAPv2, and PEAP-GTC authentication.
  - If the user manages the username and password, leave the **Username** and **Password** fields blank.
  - If all your users share the same username and password, you can input the information in the **Username** and **Password** fields.

- Enter a description in the **Password Description** field.

Note If you need to assign each user a unique username and password, you need to create a profile for each user.

Note The **Network Access Profile** field is not supported by the Cisco IP Phone 8861 and 8865.

Step 6 Click **Save**.

What to do next

Apply the WLAN Profile Group to a device pool (**System** > **Device Pool**) or directly to the phone (**Device** > **Phone**).

Set Up a Wi-Fi Group using Cisco Unified Communications Manager

You can create a wireless LAN profile group and add any wireless LAN profile to this group. The profile group can then be assigned to the phone when you set up the phone.

Procedure

Step 1 In Cisco Unified Communications Administration, select **Device** > **Device Settings** > **Wireless LAN Profile Group**.

You can also define a wireless LAN profile group from **System** > **Device Pool**.

Step 2 Click **Add New**.

Step 3 In the **Wireless LAN Profile Group Information** section, enter a group name and description.

Step 4 In the **Profiles for this Wireless LAN Profile Group** section, select an available profile from the **Available Profiles** list and move the selected profile to the **Selected Profiles** list.

When more that one wireless LAN profile is selected, the phone uses only the first wireless LAN profile.

Step 5 Click **Save**.

Configure Network Settings

Procedure

Step 1 Press **Applications** .

Step 2 To access the Network Settings menu, select **Admin settings** > **Ethernet setup**.

Step 3 Set the fields as described in Ethernet Setup Fields, on page 16.

Step 4 After you have set the fields, select **Apply** and **Save**.

Step 5 Reboot the phone.

Ethernet Setup Fields

The Network Setup menu contains fields and submenus for IPv4 and IPv6. To change some of the fields, first disable DHCP.

Establishing a VPN connection overwrites the Ethernet data fields.

Table 2: Ethernet Setup Menu Options

Entry	Type	Description
IPv4 setup	Menu	See the IPv4 Fields section. This option displays only when the phone is configured in IPv4-only mode
IPv6 setup	Menu	See the “IPv6 Fields” section.
MAC Address	String	Unique Media Access Control (MAC) address of the phone. Display only. Cannot configure.
Domain Name	String	Name of the Domain Name System (DNS) domain in which the phone re To change this field, turn off DHCP.
Operational VLAN ID		Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Ca phone is a member. This setting is blank if the auxiliary VLAN or the Administrative VLAN If the phone has not received an auxiliary VLAN, this option indicates th The phone doesn't inherit the Operational VLAN from Admin VLAN if C or Link Level Discovery Protocol Media Endpoint Discovery is enabled. To assign a VLAN ID manually, use the Admin VLAN ID option.
Admin VLAN ID		Auxiliary VLAN of which the phone is a member. Used only if the phone does not receive an auxiliary VLAN from the swit ignored.
PC VLAN		Allows the phone to interoperate with third-party switches that do not sup Admin VLAN ID option must be set before you can change this option.

Entry	Type	Description
SW port setup	Auto Negotiate 1000 Full 100 Half 10 Half 10 Full	Speed and duplex of the network port. Valid values specify: • Auto Negotiate (default) • 1000 Full:1000-BaseT/full duplex • 100 Half: 100-BaseT/half duplex • 100 Full: 100-BaseT/full duplex • 10 Half: 10-BaseT/half duplex • 10 Full: 10-BaseT/full duplex If the phone is connected to a switch, configure the switch port to the configure both to autonegotiate. Unlock network configuration options if you want to edit this setting. this option, you must change the PC Port Configuration option to the
PC port setup	Auto Negotiate 1000 Full 100 Half 10 Half 10 Full	Speed and duplex of the Computer (access) port. Valid values: • Auto Negotiate (default) • 1000 Full: 1000-BaseT/full duplex • 100 Half: 100-BaseT/half duplex • 100 Full: 100-BaseT/full duplex • 10 Half: 10-BaseT/half duplex • 10 Full: 10-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch t or configure both to autonegotiate. Unlock network configuration options if you want to change this field. must change the SW Port Configuration option to the same setting. To configure the setting on multiple phones simultaneously, enable R the Enterprise Phone Configuration window (**System** > **Enterprise P** If the ports are configured for Remote Port Configuration in Cisco Unif Administration, the data cannot be changed on the phone.

IPv4 Fields

Table 3: IPv4 Setup Menu Options

Entry	Description
DHCP Enabled	Indicates whether the phone has DHCP enabled or disabled. When DHCP is enabled, the DHCP server assigns the phone an IP address. When DHCP is disabled, the administrator must manually assign an IP address to the phone. For more information, see Set Up Phone to Use DHCP, on page 20 and Set Up Phone to Not Use DHCP, on page 21.

Entry	Description
IP Address	Internet Protocol (IP) address of the phone. If you assign an IP address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.
Subnet Mask	Subnet mask used by the phone.
Default Router	Default router used by the phone.
DNS Server 1 DNS Server 2 DNS Server 3	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2 and 3) that the phone uses.
Alternate TFTP	Indicates whether the phone is using an alternate TFTP server.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server that the phone uses. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option. 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. 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 **Note** For information about the CTL and ITL files, see the *Cisco Unified Communications Manager Security Guide*.

Entry	Description
TFTP Server 2	Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable. 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 either of the files before you can save changes to the TFTP Server 2 option. In this case, the phone deletes either of the files when you save changes to the TFTP Server 2 option. A new CTL or ITL file downloads from the new TFTP Server 2 address. If you forget to unlock the CTL or ITL file, you can change the TFTP Server 2 address in either file, then erase them by pressing Erase from the Security Configuration menu. A new CTL or ITL file downloads from the new TFTP Server 2 address. When the phone looks for the TFTP server, it 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 the following order: **1.** Any manually assigned IPv4 TFTP servers **2.** Any manually assigned IPv6 servers **3.** DHCP assigned TFTP servers **4.** DHCPv6 assigned TFTP servers **Note** For information about the CTL or ITL file, see Cisco Unified Communications Manager Security Guide.
BOOTP Server	Indicates whether the phone received the IP address from a BOOTP server rather than from a DHCP server.
DHCP Address Released	Releases the IP address that DHCP assigned. This field is editable if DHCP is enabled. If you wish to remove the phone from the VLAN and release the IP address for reassignment, set this option to Yes and press Apply.

IPv6 Fields

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 acquires and uses 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 signaling.

For more details about IPv6 deployment, see the IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.0.

You set up IPv6 from one of the following menus:

- When Wi-Fi is disabled: **Ethernet Setup** > **IPv6 setup**
- When Wi-Fi is enabled: **Wi-Fi Client Setup** > **IPv6 setup**

Use the phone keypad to enter or edit an IPv6 address. To enter a colon, press the asterisk (*) on the keypad. To enter hexadecimal digits a, b, and c, press 2 on the keypad, scroll to select the required digit, and press **Enter**. To enter hexadecimal digits d, e, and f, press 3 on the keypad, scroll to select the required digit, and press **Enter**.

The following table describes the IPv6 related information found in the IPv6 menu.

Table 4: IPv6 Setup Menu Options

Entry	Default value	Description
DHCPv6 Enabled	Yes	Indicates the method that the phone use When DHCPv6 is enabled, the phone g the IPv6-enabled router. And if DHCPv stateless (from SLAAC) IPv6 address.
IPv6 Address	::	Displays the current IPv6-only address A valid IPv6 address is 128 bits in leng • Eight sets of hexadecimal digits se • Compressed format to collapse a s colon. If the IP address is assigned with this o
IPv6 Prefix Length	0	Displays the current prefix length for th The subnet prefix length is a decimal v
IPv6 Default Router	::	Displays the default router used by the
IPv6 DNS Server 1	::	Displays the primary DNSv6 server use
IPv6 DNS Server 2	::	Displays the secondary DNSv6 server u
IPv6 Alternate TFTP	No	Allows the user to enable the use of an
IPv6 TFTP Server 1	::	Displays the primary IPv6 TFTP server
IPv6 TFTP Server 2	::	(Optional) Displays the secondary IPv6 user to set a new secondary TFTP serve
IPv6 Address Released	No	Allows the user to release IPv6-related

Set Up Phone to Use DHCP

To enable DHCP and allow the DHCP server to automatically assign an IP address to the Cisco IP Phone and direct the phone to a TFTP server, perform these steps:

Procedure

Step 1 Press **Applications** .

Step 2 Choose **Admin settings** > **Network setup** > **Ethernet setup** > **IPv4 Setup**.

Step 3 To enable DHCP, set DHCP Enabled to **Yes**. DHCP is enabled by default.

Step 4 To use an alternate TFTP server, set Alternate TFTP Server to **Yes**, and enter the IP address for the TFTP Server.

Note Consult with the network administrator to determine whether you need to assign an alternative TFTP server instead of using the TFTP server that DHCP assigns.

Step 5 Press **Apply**,

Set Up Phone to Not Use DHCP

When not using DHCP, you must configure the IP address, subnet mask, TFTP server, and default router locally on the phone.

Procedure

Step 1 Press **Applications** .

Step 2 Choose **Admin settings** > **Network setup** > **Ethernet Setup** > **IPv4 Setup**.

Step 3 To disable DHCP and manually set an IP address:

a) Set DHCP Enabled to **No**.
b) Enter the static IP address for phone.
c) Enter the subnet mask.
d) Enter the default router IP addresses.
e) Set Alternate TFTP Server to **Yes**, and enter the IP address for TFTP Server 1.

Step 4 Press **Apply**.

Load Server

Load Server is used to optimize installation time for phone firmware upgrades and offload the WAN by storing images locally, which negates the need to traverse the WAN link for each phone upgrade.

You can set the Load Server to another TFTP server IP address or name (other than the TFTP Server 1 or TFTP Server 2) from which the phone firmware can be retrieved for phone upgrades. When the Load Server option is set, the phone contacts the designated server for the firmware upgrade.

Note A Load Server option allows you to specify an alternate TFTP server for phone upgrades only. The phone continues to use TFTP Server 1 or TFTP Server 2 to obtain configuration files. The Load Server option does not provide management of the process and of the files, such as file transfer, compression, or deletion.

The Load Server is configured from the Enterprise Phone Configuration window. From Cisco Unified Communications Manager Administration, choose **Device** > **Phone** >**Enterprise Phone Configuration**.

Phone Startup Verification

After the Cisco IP Phone has power connected to it, the phone begins the startup diagnostic process by cycling through the following steps.

1. The Feature and Session buttons flash amber and then green in sequence during the various stages of bootup as the phone checks the hardware.
2. The main screen displays `Registering to Cisco Unified Communications Manager.`

If the phone completes these stages successfully, it has started up properly and the **Select** button stays lit until it is selected.

Configure Phone Services for Users

You can give users access to Cisco IP Phone Services on the IP phone. You can also assign a button to different phone services. These services comprise XML applications and Cisco-signed Java midlets that enable the display of interactive content with text and graphics on the phone. The IP phone manages each service as a separate application. Examples of services include local movie times, stock quotes, and weather reports.

Before a user can access any service:

- You must use Cisco Unified Communications Manager Administration to configure services that are not present by default.
- The user must subscribe to services by using the Cisco Unified Communications Self Care Portal. This web-based application provides a graphical user interface (GUI) for limited, end-user configuration of IP phone applications. However, a user cannot subscribe to any service that you configure as an enterprise subscription.

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

Before you set up services, gather the URLs for the sites that you want to set up and verify that users can access those sites from your corporate IP telephony network. This activity is not applicable for the default services that Cisco provides.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Services**

Step 2 Verify that your users can access the Cisco Unified Communications Self Care Portal, from which they can select and subscribe to configured services.

See Self Care Portal Management for a summary of the information that you must provide to end users.

Related Topics

Cisco Unified Communications Manager Documentation

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.

If you change an old phone with SCCP firmware to a model in the Cisco IP Phone 8800 Series, the new phone is configured for Session Line Mode.

If the old phone has a key expansion model configured, the Unified CM copies the expansion module information to the new phone at the same time. When the user connects a compatible key expansion module to the new phone, the new expansion module gets the migrated expansion module information.

If the old phone has a key expansion model configured and the new phone doesn't support an expansion module, the Unified CM doesn't copy the expansion module information.

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**.