



Cisco Unified Communications Manager phone configuration

- [Determine the MAC address of the phone, on page 1](#)
- [Install manufacturing CA certificates, on page 1](#)
- [Before you register wireless phones, on page 2](#)
- [Manual phone registration, on page 6](#)
- [Phone feature configuration, on page 10](#)

Determine the MAC address of the phone

To add a phone to the Cisco Unified Communications Manager (Unified Communications Manager), you need the media access control or MAC address of the phone.



Note The phone's MAC address is also printed on the outside of the phone's box.

Procedure

Perform one of the following actions:

- On the phone, access the **Settings** app, select **System** > **About Phone** > **Status**, and look in the Wi-Fi MAC Address field.
 - Remove the battery from the phone, and look at the label in the battery compartment of the phone.
-

Install manufacturing CA certificates

The phones use a new manufacturing certificate authority (CA). Until Cisco Unified Communications Manager (Unified Communications Manager) includes these new certificates, you must manually add the new root and intermediate certificates to the certificate chain to trust the new Manufacturing Installed Certificates (MIC).

After you add the new certificates to the trust chain, the MICs can be used for trust services such as SIP TLS, Configuration File Encryption, and LSC Certificate distribution.

Procedure

-
- Step 1** Download the missing root and intermediate certificates from the externally available [Cisco PKI](#) website. The missing certificates to complete the trust chain up to and including the root for the new MICs are:
- [Cisco Manufacturing CA III \(cmca3\)](#) - Intermediate
 - [Cisco Basic Assurance Root CA 2099 \(cbarc2099\)](#) - Root for Cisco Manufacturing CA III
- Step 2** From your web browser, log in to the **Cisco Unified Operating System Administration** web page.
- Step 3** Under the **Security** menu, select **Certificate Management**.
- Step 4** Select **Upload Certificate/Certificate Chain**.
- Step 5** Select **CallManager-trust** for the **Certificate Purpose**, browse to the certificate, then select **Upload**.
Repeat this step for all certificates on the Unified Communications Manager Publisher only as the certificate replicates to all other Unified Communications Manager nodes.
- Step 6** Select **CAPF-trust** for the Certificate Purpose, browse to the certificate, then select **Upload**.
Repeat this step for all certificates on the Cisco Unified Communications Manager publisher only.
-

Before you register wireless phones

Before you register wireless phones with your Cisco Unified Communications Manager, you can set up profiles, groups, and templates. These can simplify the phone setup when you have common information for all phones or groups of phones.





Note Auto-registration is not available for the phones.

- **Device pool**—You can create device pools to provide a common set of configurations for a group of devices.
- **Custom SIP Profile**—The phone needs a special SIP Profile, instead of the standard SIP profiles. Do not use the **Standard SIP Profile** or **Standard SIP Profile for Mobile Device**.
- **Phone button templates**—For release 1.2(0) and earlier, the phone needs a one line phone button template only.

For release 1.3(0) or later, the phone button template supports a six line phone button template. You can configure:

- Up to six multiple lines with a modifiable phone template.
- Shared lines.

- Privacy with the Privacy button option.
- **Softkey templates**—You can set up the list of features that appear on the phone **Overflow**  or **Drawer**  menu.
- **Common phone profile**—You can set up a profile for the wireless phone with the phone button and softkey templates, and then use the profile for all your wireless phones. For example, we recommend you change the default common **Local Phone Unlock Password** from ****#** to a more secure password.
- **Phone security profile**—You can create a custom security profile if the default or existing phone security profiles do not cover your needs.

You can find detailed instructions about these profiles and templates in the [System Configuration Guide for Cisco Unified Communications Manager](#) for your release.

Device pool configuration

Configure device pools for the phones based on your organization's requirements. For example, you may want to create device pools that are based on phone locations or phone models and that define the following settings.

- Device settings (such as **Cisco Unified Communications Manager Group**)
- Roaming sensitive settings (such as **Date/Time Group**, **Region**, and so on)
- Local route group settings
- Device mobility-related information settings

Create custom SIP profile

Cisco Unified Communications Manager has standard SIP profiles available. However, a custom SIP Profile for your wireless phones is the preferred profile.

Procedure

-
- Step 1** From the Cisco Unified Communications Manager Administration web page, select **Device > Device Settings > SIP Profile**.
- Step 2** Click **Find**.
- Step 3** Click the **Copy** icon beside **Standard SIP Profile**.
- Step 4** Set the name and description. For example:
- Custom 840 SIP Profile**
- Custom 860 SIP Profile**
- Step 5** Set these parameters.
- **Timer Register Delta (seconds)**—Set to 30 (default is 5).
 - **Timer Keep Alive Expires (seconds)**—Set to 300 (default is 120).

- **Timer Subscribe Expires (seconds)**—Set to 300 (default is 120).
- **Timer Subscribe Delta (seconds)**—Set to 15 (default is 5).

Note Ensure **SIP Station KeepAlive Interval** at **System > > Service Parameters > > Cisco CallManager** remains configured for 120 seconds.

Step 6 Click **Save**.

Phone button template configuration

Configure a Phone Button Template for the phones. For release, 1.2(0) or earlier, the phones support a one line phone button template only.

For release 1.3(0) or later, the phones support up to six lines and shared lines. By default, the phone button template has buttons 1 and 2 set to **Line** and buttons 3–6 set to **None**. You can create customer phone templates to add multiple lines or privacy on shared lines to any of the 6 buttons.

For details, see the *System Configuration Guide for Cisco Unified Communications Manager* and the *Feature Configuration Guide for Cisco Unified Communications Manager* for your Cisco Unified Communications Manager release, at [Configuration Guides](#).

Phone softkey templates

Phones download softkey configuration files from Cisco Unified Communications Manager (Unified Communications Manager). At initial release, you can use the Softkey Template to allow or prevent the appearance of the following features in the Cisco Phone app Overflow menu:

- Call Forward
- Call Park
- iDivert
- Hunt Group Login/Logout

Any other Softkey Template configuration setting is not supported currently.

In the Cisco Unified Communications Manager Softkey Layout Configuration page, there are Softkey options for 12 different call states. Some call state examples are: On hook, Connected, On Hold, Ring In, Off Hook, Connected Transfer, and Digits After First.

On a phone, if the Call Forward, Call Park, iDivert, and Hunt Group Login/Logout options are configured as Selected Softkeys in any of the 12 call states, the phone presents the Overflow menu features only in appropriate call states. For example, even if configured, the Call Park feature isn't presented to the user if there are no active calls. However, if Call Park isn't in the Selected Softkeys list for any of the Softkey profiles, it isn't offered to the user in any call state.

For details, refer to the [System Configuration Guide for Cisco Unified Communications Manager](#) for your Unified Communications Manager release.

Create a new phone security profile

You must have a phone security profile for your phones. You can either:

- Use the default Phone Security Profile in the Cisco Options Package (COP) file:
 - Cisco 840 Standard SIP Non-Secure Profile**
 - Cisco 860 Standard SIP Non-Secure Profile**
- Use an existing Phone Security Profile if it conforms to the following recommended values.
- Create a unique Phone Security Profile for the Cisco Wireless Phone 840 and 860.



Note The Certificate Authority Proxy Function (CAPF) must be operational to use a Locally Signed Certificate (LSC) with a security profile. The phones have a Manufacturing Installed Certificate (MIC), which can be used with a security profile as well.



Note Each deployment is unique and may require options other than the following recommendations due to site policy or administrative requirements.

Procedure

-
- Step 1** In the Cisco Unified Communications Manager Administration web page, select **System > Security > Phone Security Profile**.
- Step 2** Click **Add New**.
- Step 3** Select the phone model:
- Cisco 840**
 - Cisco 860**
- Step 4** Click **Next**.
- Step 5** On the **Phone Security Profile Information** pane, set these parameters:
- **Name**—Give the new profile a name, such as Cisco 860 – Encrypted with Digest Authentication.
 - **Device Security Mode**—Select an option:
 - Note** We do not currently support the **Authenticated** device security mode.
 - **Encrypted**—For TLS and SRTP.
 - **Non Secure**—To use UDP or TCP.
 - **Transport Type**—Select an option:
 - Note** We do not recommend the **UDP** option, due to port connectivity issues. If you choose **TCP+UDP**, only TCP is used.

- **TLS**—Use with Authenticated or Encrypted Device Security Mode. We recommend TLS for enhanced security.
- **TCP**—Use with Nonsecure Device Security Mode for reliable packet delivery.
- **Enable Digest Authentication**— Select the check box to configure the phone with Digest Authentication.
- **TFTP Encrypted Config**—Select the check box for enhanced security if you are using the Cisco Wireless Phone Configuration Management tool to create a configuration file for the phone.

Note Leave the other fields at their Defaults.

Step 6 (Optional) To help deploy LSC certificates to your devices, complete the **Phone Security Profile CAPF Information** pane.

For details, refer to the [Security Guide for Cisco Unified Communications Manager](#) for your Cisco Unified Communications Manager release.

Note We do not support 512-bit keys.

Step 7 Click **Save**.

Manual phone registration

When a new phone is added to your network, manual phone registration means that you need to configure the phone in your call control system. The configuration includes the directory number, information about the user, and the phone profile.

After you configure the phone in the call control system, you configure the phone to connect to the call control system.

Add an end user (Optional)

It is optional to add an end user. However, you must add an end user to:

- Provide the user access to the Self Care portal.
- Allow the user to appear in the corporate directory.
- Allow you to configure security profiles that include Digest Authentication.

Procedure

Step 1 From the Cisco Unified Communications Manager Administration web page, select **User Management > End User**.

Step 2 Click **Add New**.

Step 3 In the **User Information** section, set the following parameters:

- **User ID**—Enter a user ID that complies with your system and account policies.

- **Password**—Enter a password for this user that complies with your system and account policies. If your system is LDAP integrated, this field is dimmed and unavailable. In this case, you can create or modify this password through the Active Directory Server.
- **Confirm Password**—Repeat the password.
- (Optional) **Self Service-User ID**—Use the extension number for the device.
- (Optional) **Pin**—Enter a pin to let the end user use pin enabled features such as user web login.
- **Confirm Pin**—Repeat the pin.
- **Last Name**—Enter the User's last name.
- **First Name**—Enter the User's first name.
- **Digest Credentials**—Enter the Digest Authentication Password that you would like the phone to use to register.
- **Confirm Digest Credentials**—Repeat the Digest Authentication Password.

Note Enter other **End User** field values as required by your site's system and account policies.

Step 4 Click **Save**.

Add the phone

Before the phone can be used, you add it to the Cisco Unified Communications Manager (Unified Communications Manager) and assign it to a user.

Before you begin

Install the following files on the Unified Communications Manager:

- Latest device enabler QED installer Cisco Options Package (COP) file
- Latest phone software COP file

Get the MAC address of the phone.

Procedure

- Step 1** From the Cisco Unified Communications Manager Administration web page, select **Device > Phone**.
- Step 2** Click **Add New**.
- Step 3** Select the phone model:
- Cisco 840**
 - Cisco 860**
- Step 4** Click **Next**.
- Step 5** In the **Device Information** section, set the following minimal phone information:

Note These minimal settings allow users to make and receive calls. Enter other fields as required by your site policies and procedures for new phone additions.

- **MAC Address**—Enter the MAC address of the phone. You can enter the address with lowercase letters. This value must match the WLAN MAC address of the physical phone that is registering to this Unified Communications Manager.
- (Optional) **Description**—Enter a meaningful description; for example, the user's name and phone model.
- **Device Pool**—Select the appropriate pool of phones. The device pool defines common settings such as the Cisco Unified Communications Manager Group, local route group settings, device mobility-related information settings, and other group settings. It's helpful to use Device Pools to group devices by location or model.
- **Phone Button Template**—Select the appropriate template.
- **Softkey Template**—Select the appropriate template.

Caution This window lists all the Softkeys in the system although not all phones support all Softkeys. If you choose a Softkey that is not supported by the phone, the Softkey won't display on the phone even if you configured it in this list.

- **Calling Search Space**—Select the appropriate space for the phone. The Calling Search Space determines how, and if, to route a dialed number. Configure the Calling Search Space so that it routes to any numbers that are part of your dial plan.
- **Location**—Select the desired location for the phone.
- **Owner User ID**—Select an option:
 - If you want to assign the phone to an End User, select the desired End User.
 - If you don't want to associate the phone to an End User, select **Anonymous**.
- **Allow Control of Device from CTI**—Select the check box to allow control of device from CTI.

Step 6 In the **Protocol Specific Information**, set the following minimal information:

- **Device Security Profile**—Select the desired Phone Security Profile.
- **Re-routing Calling Search Space**—Select a Calling Search Space with permissions appropriate for dialing any call forward or transfer destination that you may use.
- **SIP Profile**—Select **Standard SIP Profile**.
- **Digest User**—Select an option:
 - If you chose a Device Security Profile that includes Digest Authentication, select the desired end-user ID.
 - If you chose a Device Security Profile that doesn't include Digest Authentication, select **None**.
- Click **Save** and **OK**.

Step 7 In the **CAPF** section, select **CAPF** to allow CAPF and allow you to install and upgrade the phone's certificate.

Step 8 Click **Save** and **OK**.

Add the phone extension

For release 1.2(0) or earlier, the phone supports a single line only, which can't be a shared line.

For release 1.3(0) or later, the phone supports up to six lines, including shared lines.

At a minimum, configure the following fields on the Directory Number Configuration window. If required by your site policies and procedures for new extension provisioning, you may need to configure more fields.

Before you begin

Add the phone.

Procedure

Step 1 From the Cisco Unified Communications Manager Administration Phone Configuration page, click **Line [1] – Add a new DN**.

Step 2 In the **Directory Number Information** section, set the following:

- **Directory Number**—Enter the Extension number, or Directory Number for the phone.
- **Description**—Enter a description for this particular Directory Number.
- **Alerting Name**—Enter a name that displays to callers.
- **ASCII Alerting Name**—Enter the same name from the Alerting Name field.

Step 3 In the **Directory Number Settings** section, set the following:

- **Voice Mail Profile**—If this Directory Number uses voicemail, select a profile that directs callers to the voicemail pilot number. For example, select the `Cisco_Unity_Connection_Profile`.
- **Calling Search Space**—Select a Calling Search Space with partitions that include any numbers you may dial from this line.

Step 4 In the **Call Forward and Call Pickup Settings** section, set the Call Forward Settings as desired for your environment. For example, you can configure Call Forward for all unavailable, no answer, or busy scenarios to forward calls to the Cisco Unity Connection Voicemail server. Or you may also specify a different, unique call forward **Destination**.

Caution If Cisco Unified Communications Manager is using Partitions and Calling Search Spaces, we recommend that you configure the **Call Forward Calling Search Spaces**. Failure to configure a Call Forward Calling Search Space may result in call forward failures.

Step 5 In the **Line 1 on Device** section, set the following:

- **Display**—Enter the name to present to internal called parties.
- **ASCII Display**—Enter the same name from the Display field.

- **Line Text Label**—Enter the line text label.
- **External Phone Number Mask**—Enter the external phone number mask.
- **Recording Option**—Choose one of the following options. Default is **Call Recording Disabled**.
 - **Call Recording Disabled**
 - **Automatic Call Recording Enabled**
 - **Selective Call Recording Enabled**
- **Recording Profile**—Select the recording profile from the options after enabling call recording option. Default is **< None >**.
- **Recording Media Source**—Select one of the following options. Default is **Gateway Preferred**.
 - **Gateway Preferred**
 - **Phone Preferred**
- **Monitoring Calling Search Space**—Select one of the following options. Default is **< None >**.
 - **<None>**
 - **Auto_register**

Step 6 In the **Multiple Call/Call Waiting Settings on Device** section, set the following:

- **Maximum Number of Calls**—Enter 4. Four calls are the maximum number of calls the phone can place or receive per registration.
- **Busy Trigger**—Enter 4. Four calls are the maximum number of calls the phone can place or receive per registration.

Step 7 Click **Save**.

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)

For example, if you don't want a specific set of users to access the phone Web pages, but the rest of your users can access the pages, you:

1. Enable access to the phone web pages for all users.
2. Disable access to the phone web pages for each individual user, or set up a user group and disable access to the phone web pages for the group of users.
3. If a specific user in the user group did need access to the phone web pages, you could enable it for that particular user.

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 Layout fields

The following table describes the fields in the Product Specific Configuration Layout pane.

Table 1: Product Specific Configuration Layout fields

Field name	Field type or choices	Default	Description
Web Access	Disabled Enabled	Disabled	Enables or disables access to the phone web pages through a web browser. Caution If you enable this field, you may expose sensitive information about the phone.
Web Password			Specifies the password to access the phone's Web interface. Enter a 8-127 character password.
Reboot immediately after downloading software updates	Disabled Enabled	Disabled	Specifies whether the phone reboots immediately after downloading a software update or if the phone notifies the user to manually reboot. To apply software updates, the phone must be rebooted.
Emergency Numbers	String of up to 16 characters, comma separated, no spaces		Sets the list of emergency numbers that the users see when they try to dial without signing in. Example: 911,411,511
Visual Voicemail Access	Disabled Enabled	Disabled	Controls access to Visual Voicemail.
Voicemail Server (Primary)	String of up to 256 characters		This parameter contains the address of the primary voicemail server for Visual Voicemail.

Field name	Field type or choices	Default	Description
Voicemail Server (Backup)	String of up to 256 characters		This parameter contains the address of the backup voicemail server for Visual Voicemail.
Load Server	String of up to 256 characters		Identifies the alternate IPv4 server that the phone uses to obtain firmware loads and upgrades. The load server uses HTTP on TCP port 6970. It doesn't support TFTP on UDP port 69.
Advertise G.722 and Opus Codecs	Use System Default Disabled Enabled	Use System Default	<p>Indicates whether the phone advertises the G.722 and Opus codecs to the Cisco Unified Communications Manager (Unified Communications Manager).</p> <ul style="list-style-type: none"> • Use System Default—Defers to the setting specified in the enterprise parameter Advertise G.722 Codec. • Disabled—Does not advertise G.722 or Opus to the Unified Communications Manager. • Enabled—Advertises G.722 and Opus to the Unified Communications Manager. <p>Note Codec negotiation involves two steps:</p> <ol style="list-style-type: none"> 1. The phone must advertise the supported codec to the Unified Communications Manager (not all endpoints support the same set of codecs). 2. When the Unified Communications Manager gets the list of supported codecs from all phones that are involved in the call attempt, it chooses a commonly supported codec based on various factors, including the region pair setting.
Customer support upload URL	String of up to 256 characters		Identifies the location that the phones use to upload problem reporting tool (PRT) output files.
Secondary SIP Server			<p>This parameter contains the address of the server for the optional second registration.</p> <p>Note The purpose of the Secondary SIP Server is to allow registration of a SIP line to a separate SIP server, such as a Nurse-call system integration. It is not intended as a failover or redundancy solution.</p>

Field name	Field type or choices	Default	Description
Secondary SIP Server Port			Identifies the far-end port number for the optional second registration.
Secondary SIP Transport	UDP TCP TLS	UDP	Identifies the transport type for the optional second registration.
Secondary SIP Extension			Identifies the SIP extension for the optional second registration.
Secondary SIP Username			Identifies the SIP username for the optional second registration.
Secondary SIP Password			Identifies the SIP password for the optional second registration.
Enterprise Mobility Management (EMM) Alternative Configuration	String of up to 256 characters		Identifies the name of the configuration filename created in the Cisco Wireless Phone Configuration Management tool and added to Cisco Unified Communications Manager TFTP nodes. If the file is encrypted, the format is config.json.enc . If the file isn't encrypted, the format is config.json . Don't use unencrypted files on your production server, use only for troubleshooting.
Enterprise Mobility Management (EMM) Alternative Configuration Encryption Key	String of 64 characters		Identifies the key if using an encrypted configuration file created in the Cisco Wireless Phone Configuration Management tool. The key.txt file contains the encryption key. Blank if the file isn't encrypted.
Recording Tone	Enabled Disabled	Enabled	Specifies whether to get recording warning tone while recording the call. <ul style="list-style-type: none"> • Disabled— Unmutes the recording warning tone. • Enabled— Mutes the recording warning tone.
Announce Caller ID	Disabled Enabled Headset Only	Disabled	Specifies whether to announce the Caller ID. <ul style="list-style-type: none"> • Disabled—Does not announces the Caller ID. • Enabled—Announces the Caller ID on the phone. • Headset Only—Announces the Caller ID Only when using a headset.
Mute SIP Registration Notifications	Disabled Enabled	Disabled	Specifies whether to receive SIP Registration Notifications.

Field name	Field type or choices	Default	Description
Line 1 Ringtone		Flutey Phone	Specifies the Line 1 Ringtone. Note By selecting a "None" type ringtone, the phone doesn't ring, but displays the incoming calls.
Line 2 Ringtone		Flutey Phone	Specifies the Line 2 Ringtone. Note By selecting a "None" type ringtone, the phone doesn't ring, but displays the incoming calls.
Line 3 Ringtone		Flutey Phone	Specifies the Line 3 Ringtone. Note By selecting a "None" type ringtone, the phone doesn't ring, but displays the incoming calls.
Line 4 Ringtone		Flutey Phone	Specifies the Line 4 Ringtone. Note By selecting a "None" type ringtone, the phone doesn't ring, but displays the incoming calls.
Line 5 Ringtone		Flutey Phone	Specifies the Line 5 Ringtone. Note By selecting a "None" type ringtone, the phone doesn't ring, but displays the incoming calls.
Line 6 Ringtone		Flutey Phone	Specifies the Line 6 Ringtone. Note By selecting a "None" type ringtone, the phone doesn't ring, but displays the incoming calls.

Field name	Field type or choices	Default	Description
	None		
	Andromeda		
	Aquila		
	Argo Navis		
	Atria		
	Beat Plucker		
	Bell Phone		
	Big Easy		
	Canis Major		
	Carina		
	Cassiopeia		
	Centaurus		
	Chimey Phone		
	Cygnus		
	Digital Phone		
	Ding		
	Draco		
	Dream Theme		
	Eridani		
	Flutey Phone		
	Free Flight		
	Girtab		
	Growl		
	Hydra		
	Insert Coin		
	Kuma		
	Lyra		
	Machina		
	Mildly Alarming		
	New Player		
	Noisey One		
	Orion		
	Pegasus		

Field name	Field type or choices	Default	Description
	Perseus Pyxis Rasalas Rigel Scarabaeus Sceptrum Solarium Testudo Third Eye Very Alarmed Vespa Zeta		
Notification Sound			Specifies the notification sound files to download. Multiple files can be specified using the comma separated format. Once the files have been downloaded, the notification sound will need to be configured via the Custom Settings application, Android Settings, or in other application settings.
Alarm Sound			Specifies the alarm sound files to download. Multiple files can be specified using the comma separated format. Once the files have been downloaded, the alarm sound will need to be configured via the Custom Settings application, Android Settings, or in other application settings.
Wallpaper			Specifies the wallpaper files to download. Multiple files can be specified using the comma separated format. Once the files have been downloaded, the lock screen wallpaper and home screen wallpaper will need to be configured via the Custom Settings application or Android Settings.

Related Topics

[Cisco app software updates](#)

Configure visual voicemail

Configuration and use of visual voicemail is optional. By default, the visual voicemail feature is disabled. With visual voicemail disabled, users may access, listen to, and delete their voicemail messages through the Cisco Unity Connection IVR just as they would with any other Cisco handset. However, if you enable visual voicemail, its UI gives users a much easier to use interface to manage their voicemails than the dial-in IVR.

Procedure

- Step 1** To allow TLS connections from the device to the Cisco Unity Connection server, verify that the server's tomcat-trust certificate is in Cisco Unified Communications Manager's tomcat-trust certificate trust list.
- Step 2** From the Cisco Unity Administration page, configure the Voicemail box and Web application password for the user.
- Step 3** From the Cisco Unified Communications Manager Administration web page, set the Visual Voicemail Access field for the device to **Enabled**.
- Step 4** From the Cisco Unified Communications Manager Administration web page, configure the Voicemail Server (Primary) address to point to the integrated Cisco Unity Connection server.
-

Configure Tomcat trust certificate

Export the tomcat-trust certificate from the Cisco Unity Connection server and import it as a tomcat-trust certificate to Cisco Unified Communications Manager.

Procedure

- Step 1** Export the certificate from Cisco Unity Connection:
- On the Cisco Unity Connection server, navigate to **Cisco Unified OS Administration**.
 - Navigate to **Security > Certificate Management**.
 - Select the certificate labeled **tomcat-trust**.
 - Choose to download the .pem file.
- Step 2** Import the certificate to each Cisco Unified Communications Manager in the cluster.
- On the Cisco Unified Communications Manager server, navigate to **Cisco Unified OS Administration**.
 - Navigate to **Security > Certificate Management**.
 - Click **Upload Certificate/Certificate Chain**.
 - From the **Certificate Purpose** drop-down list, choose **tomcat-trust**.
 - Enter a **Description** for the certificate, such as **tomcat-trust**.
 - Click **Browse** to search for, and select, the certificate.
 - Click **Upload**.
- Step 3** Restart the Tomcat service for the changes to take effect.

Note You must restart the Tomcat service for the new certificate to be available to the phone when it validates the TLS connection to Cisco Unity Connection.

Configure the voicemail box and Web Application Password

Configure a mailbox for the user on the Cisco Unity Connection server as you would for any other user. However, while users may know their voicemail PIN, it may differ from their Web Application Password; which is what the Cisco Wireless Phone 840 and 860 visual voicemail feature uses to access their messages. Set the user's Web Application Password.

Procedure

- Step 1** In the Cisco Unity Connection system, navigate to **Users > Users**, and select the user.
- Step 2** Under Choose Pin, use the pulldown to select the **Web Application** box.
- Step 3** Unselect the **User must change at Next Sign-In** box if currently selected (the Cisco Wireless Phone 840 and 860 does not currently provide a mechanism to change the password through the phone's UI).
- Step 4** Using the top pull-down menu, select **Edit > Change Password > .**
- Step 5** In the Choose Password pulldown, select **Web Application**.
- Step 6** Enter a Password.
- Set the Password to something that will conform to your Site's Authentication rules. This value must match the value that the user enters in the **Enter Unity Web Credentials** dialog box that appears when they navigate to the Voicemail tab in the **Cisco Phone** app.
- Step 7** Select **Save**.
- Step 8** Give the user's Unity Alias and Web Application Password to the user, so they can enter them in the Unity Web Credentials dialog box when prompted.
-

Enable Visual Voicemail Access

For the Voicemail tab to appear on the user's device, you must enable **Visual Voicemail Access** on the Phone Configuration page of the device.

If the **Visual Voicemail Access** is set to **Disabled**, the Voicemail tab does not appear on the user's devices.

Procedure

- Step 1** From the Cisco Unified Communications Manager Administration web page, select **Device > Phone**.
- Step 2** Select the device you want to configure.
- Step 3** In the Product Specific Configuration Layout portion of the Phone Configuration Page for the device, set **Visual Voicemail Access** to **Enabled**.
-

Configure the voicemail server to the Cisco Unity Connection server

Provision the voicemail server address in the Cisco Unified Communications Manager, so the phones can locate the Cisco Unity Connection server.

Procedure

Choose one of the following methods:

- Configure the Voicemail Server (Primary) and Voicemail Server (Backup) IP addresses as part of a Common Phone Profile Configuration for the devices at an Enterprise level under **System > Enterprise Phone Configuration**.

- **a.** Configure the Voicemail Server (Primary) and Voicemail Server (Backup) IP addresses as part of a Common Phone Profile Configuration for individual devices in Cisco Unified CM Administration **Device > Phone**.
- b.** Select the device you want to configure.
- c.** From the Product Specific Configuration Layout portion of the Phone Configuration Page of the device:
 - Set the Voicemail Server (Primary) field to the address of your main Cisco Unity Connection server.
 - If available, set the Voicemail Server (Backup) field to the address of your backup Cisco Unity Connection server.

Phone services

You can provide your users with special phone services. Before a user can access any service, you must configure the services with Cisco Unified CM Administration.

With release 1.3(0) or later, extension mobility is available for the phones. To configure extension mobility, see the Extension Mobility chapter in the [Feature Configuration Guide for Cisco Unified Communications Manager](#) for your release.

With release 1.4(0) or later, extension mobility cross cluster (EMCC) is available for the phones. To configure EMCC, see the Extension Mobility Cross Cluster chapter in the [Feature Configuration Guide for Cisco Unified Communications Manager](#) for your release.

With release 1.6(0) or later, Webex Calling is supported for phones. To configure Webex Calling feature to your phone, see <https://help.webex.com/ld-nzid8xi>

Supports the following Webex Standard Call features:

Call Waiting
Call Hold and Resume
Call Transfer
Call Park
Multiline
Shared Call appearance
Support Standard SIP timers on Call duration
Media Codec Support – G.711a, G.711u, G.729a, G.722, OPUS
Message Waiting Indicator signaled by unsolicited SIP notify
Call quality Metrics/Reports on call termination (SIP Bye message)

Serviceability support through PRT trigger & Packet Capture · Call Recording
--

E-911/RedSky integration – Held support

For release 1.7(0) or later, Lightweight Directory Access Protocol (LDAP) feature is available for the phones in Webex Calling. It allows you to program NFC card with the audio profiles and use NFC card to copy the profile(s) to other devices.

With release 1.9(0) or later, Cisco Unified SRST feature is available for the phones. When a WAN link fails, the phone loses connection with the central CUCM, but the phone immediately registers with a local Cisco Unified SRST gateway. It detects newly registered wireless phones, queries these phones for their configuration, and then autoconfigures itself.

Cisco Wireless Phone 840 and 860 support the following Cisco Unified SRST features:

Auto answer	Line label
Attended transfer	Multiple lines
Call forward	Redial
Call waiting	Secure SRST
Conference	Speed dial
Do not disturb	SRST failover and failback
Hold/Resume	Voice hunt group

Phone line configuration options

For release 1.3(0) or later, you can configure Auto Answer and Line Text Label for the Cisco Wireless Phone 840 and 860.

For more details about these options, see the [Feature Configuration Guide for Cisco Unified Communications Manager](#) for your release.

For release 1.8(0) or later, you can configure Recording Option, Recording Profile, and Recording Media Source for the Cisco Wireless Phone 840 and 860.

Problem report tool

The **Report a Problem** feature on the **Cisco Phone** app creates a problem report log bundle. To troubleshoot phone problems, you require:

- The log bundles from the **Report a Problem** feature.
- The date and time of the problem.
- A description of the problem.

If the phone's web browser is enabled, you can download the log bundle from the phone's web browser.

Optionally, you may set up a problem report upload server for the log bundles. To set up a problem report upload server, you must add a server address to the Customer Support Upload URL field on Cisco Unified Communications Manager.

Related Topics

[Problem report log bundles](#)

Configure a customer support upload URL

You must use a server with an upload script to receive PRT files. The PRT uses an HTTP POST mechanism, with the following parameters included in the upload (utilizing multipart MIME encoding):

- devicename (example: “SEP001122334455”)
- serialno (example: “FCH12345ABC”)
- username (the username configured in Cisco Unified Communications Manager, the device owner)
- prt_file (example: “probrep-20141021-162840.tar.gz”)

A sample script is shown below. This script is provided for reference only. Cisco does not provide support for the upload script installed on a customer's server.

```
<?php
// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used: upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
    header("HTTP/1.0 500 Internal Server Error");
    die("Error: You must select a file to upload.");
}

?>
```

Procedure

-
- Step 1** Set up a server that can run your PRT upload script.

- Step 2** Write a script that can handle the parameters listed above, or edit the provided sample script to suit your needs.
- Step 3** Upload your script to your server.
- Step 4** In Cisco Unified Communications Manager, go to the Product Specific Configuration Layout area of the individual device configuration window, Common Phone Profile window, or Enterprise Phone Configuration window.
- Step 5** Check **Customer support upload URL** and enter your upload server URL.
- Example:**
http://example.com/prtscript.php
- Step 6** Save your changes.
-

Corporate and personal directories setup

You can make it easy for your users to contact coworkers using a corporate directory.

You can also enable users to create personal directories. Each individual user has a personal directory, which they can access from any device.

The corporate and personal directories are set up in the Cisco Unified Communications Manager.

Corporate directory setup

The Corporate Directory allows a user to look up phone numbers for coworkers. To support this feature, you must configure corporate directories.



Cisco Unified Communications Manager uses a Lightweight Directory Access Protocol (LDAP) directory to store authentication and authorization information about users of Cisco Unified Communications Manager applications that interface with Cisco Unified Communications Manager. Authentication establishes user rights to access the system. Authorization identifies the telephony resources that a user is permitted to use, such as a specific phone extension.

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

After you complete the LDAP directory configuration, users can use the Corporate Directory service on their phone to look up users in the corporate directory.

Personal directory setup

The personal directory allows a user to store a set of personal numbers in their Personal Address Book (PAB). Access the personal directory from the:

- Cisco Unified Communications Self Care Portal on a web browser—Provide users with the URL and login credentials.
- **Contacts**  tab on the **Cisco Phone**  app—Provide users login credentials.

Self Care Portal overview

From the Cisco Unified Communications Self Care Portal, users can customize and control phone features and settings.

As the administrator, you control access to the Self Care Portal. You must also provide information to your users so that they can access the Self Care Portal.

Before a user can access the Cisco Unified Communications Self Care Portal, you must use Cisco Unified Communications Manager Administration to add the user to a standard Cisco Unified Communications Manager End User group.

You must provide end users with the following information about the Self Care Portal:

- The URL to access the application. This URL is:
`https://<server_name:portnumber>/ucmuser/`, where `server_name` is the host on which the web server is installed, and `portnumber` is the port number on that host.
- A user ID and default password to access the application.
- An overview of the tasks that users can accomplish with the portal.

These settings correspond to the values that you entered when you added the user to Cisco Unified Communications Manager.

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

Set up user access to the Self Care Portal

Before a user can access the Self Care Portal, you need to authorize the access.

Procedure

-
- Step 1** In Cisco Unified Communications Manager Administration, select **User Management > End User**.
 - Step 2** Search for the user.
 - Step 3** Click the user ID link.
 - Step 4** Ensure that the user has a password and PIN configured.
 - Step 5** In the Permission Information section, ensure that the Groups list includes **Standard CCM End Users**.
 - Step 6** Select **Save**.
-

Call pickup

Cisco Unified Communications Manager Call Pickup allows user to pick up call from other phones when the phone is busy or in a call queue or shared line group, a call comes into user's phone. For example, a user can still pick up the phone from someone's desk.

- **Pickup:** A phone that is assigned to a pickup group and can answer a call ringing on another phone in its own group. To activate, press the **Pickup** softkey.