



Phone configuration

- [Enterprise Mobility Management application configuration, on page 1](#)
- [Cisco Wireless Phone Configuration Management tool , on page 2](#)
- [Manual phone configuration, on page 10](#)

Enterprise Mobility Management application configuration

We recommend that you configure an Enterprise Mobility Management (EMM) application and generate a QR code to program the phones to connect to WLAN and EMM application. When each phone enrolls with the EMM application, it receives the phone apps, certificates, and configuration for all non-Cisco Unified Communications Manager related functionality.

Enroll the phones to the Enterprise Mobility Manager application

Enroll the phones to the Enterprise Mobility Management (EMM) application through the device owner method.

See your EMM application documentation for additional information.

Before you begin

Ensure that the battery is fully charged.

Ensure that you allow the following apps:

- Cisco Phone: com.cisco.phone
- System Updater: com.cisco.sysupdater
- UCM Client: com.cisco.ucmclient
- Logging: com.cisco.logging
- Application URLs: com.cisco.appurl
- Port Manager: com.cisco.portmanager



Note You may need to add the Google Keyboard (Gboard) app, based on your EMM application. There are also several Cisco apps that are on the Google Play Store you may want to add.

Procedure



- Step 1** Press and hold the **Power** button until the phone vibrates and the first screen displays.
 - Step 2** On the startup screen, quickly tap the display six times.
 - Step 3** Scan a QR code.
-

Related Topics

[Cisco app package names](#)

Cisco Wireless Phone Configuration Management tool

If you don't use an Enterprise Mobility Management (EMM) application to configure your phones, we recommend that you use the [Cisco Wireless Phone Configuration Management](#) tool. The Cisco Wireless Phone Configuration Management tool Deployment Configuration tab has two apps to allow you to restrict access to apps and settings.

- The **Smart Launcher**  app allows you to specify which apps to display on the home launcher screen. You can configure these modes:
 - Single-app mode—Specify a single app, such as the Cisco Phone app, to display on the Smart Launcher. Other apps aren't available to the user.
 - Multiple-app mode—Specify multiple apps to display on the Smart Launcher. Other apps aren't available to the user.
- The **Device Policy Controller**  app allows you to disallow apps on the phone to prevent users from getting to an app that isn't on their launcher screen through another app. For example, if the user clicks a link to a website that they receive in a Webex message, the link opens in a browser if the Chrome app isn't in the disallowed list.

The Cisco Wireless Phone Configuration Management tool also allows you to change or lock down settings for the various Cisco apps.




Note To use the configuration file that is generated by the utility and loaded into Cisco Unified Communications Manager (CUCM), the administrator must perform the following:

1. Reset the phone to factory settings.
2. Generate the QR code using the Initial Provisioning tab in the configuration tool.
3. Scan the QR code.

*Failure to scan the QR code to onboard the phone prevents the phone from downloading the configuration file from CUCM when it has joined the wireless network and registered to CUCM.

In Smart Launcher mode, the phone has only these four Quick Settings: Display brightness, Flashlight, Volume controls, and Exit Launcher. However, the notification shade also presents the gear icon to open the Android settings app. We recommend that you disallow the **Allow Notification Shade Settings Gear** in the Custom Settings app in Cisco Wireless Phone Configuration Management tool. Otherwise, you can easily open apps that aren't on the Smart Launcher.



Note Access the Quick Settings from the notification shade in single-app mode, or in the **Overflow**  menu in multiple-app mode.

Cisco Wireless Phone Configuration Management tool workflow

You use the Cisco Wireless Phone Configuration Management tool to:

- Generate a QR code to enroll your phones to the call control system.
- Create an encrypted configuration file to allow and restrict certain apps and settings on the phones.

Procedure

	Command or Action	Purpose
Step 1	Enable TFTP encryption in the Phone Security Profile, so that the configuration data sent to the phones through TFTP isn't in cleartext format.	See Create a new phone security profile .
Step 2	Update the default Local Phone Unlock Password of **# so that users can't exit the Smart Launcher and access more settings or apps.	Change the password in the Cisco Unified CM Administration web page under Device > Device Settings > Common Device Profile .
Step 3	Install the 1.5 software on the phones.	See Load the COP files to Cisco Unified Communications Manager .
Step 4	Factory reset the phones.	See Reset to factory default through the phone settings .

	Command or Action	Purpose
Step 5	In the Deployment Configuration tab of the Cisco Wireless Phone Configuration Management tool, generate an encrypted phone configuration file.	See Create encrypted phone configuration file, on page 5 .
Step 6	Upload the phone configuration file to Cisco Unified Communications Manager.	See Upload the phone configuration file to Cisco Unified Communications Manager, on page 9 .
Step 7	In the Initial Provisioning tab of the Cisco Wireless Phone Configuration Management tool, generate a QR code.	See Generate a QR code to initialize phones, on page 4 .
Step 8	Enroll the phones with the QR code.	See Enroll phones with Cisco Wireless Phone Configuration Management tool QR code, on page 5 .
Step 9	Restart the phones before you give them to users.	
Step 10	(Optional) You can update existing phone configuration files by importing the zip file into the Cisco Wireless Phone Configuration Management tool.	See Update existing configuration file, on page 9 .

Generate a QR code to initialize phones

With the Cisco Wireless Phone Configuration Management tool, you generate a Quick Response (QR) code to connect the phones with the WLAN and Cisco Unified Communications Manager.

You can generate and save as many different QR codes as you need for your organization.



Note After you generate a QR code, we recommend that you save it as a PDF or other scannable source, so that you can reuse it.

Before you begin

Get your Wi-Fi credentials, if applicable.

Procedure

-
- Step 1** From any browser, open the [Cisco Wireless Phone Configuration Management tool](#).
- Step 2** Click the **Initial Provisioning** tab.
- Step 3** Choose one of these **Security** options.
- **None**
 - **WPA-Personal**

- WPA-Enterprise

- Step 4** Enter the **SSID** and, if necessary, **Password**.
- Step 5** Click **Generate**.
- Step 6** Keep the QR code open or save it, so you can use it to enroll the phones.
-

Enroll phones with Cisco Wireless Phone Configuration Management tool QR code

To enroll the phones with the Cisco Wireless Phone Configuration Management tool QR code, the phone must be in range of the Wi-Fi network.

Before you begin

- Update the phone software to release 1.5(0) and then factory reset the phone.
- Generate the Cisco Wireless Phone Configuration Management tool QR code.

Procedure



- Step 1** On the **Hi there** startup screen, quickly tap the display six times.
The camera opens.
- Step 2** Center the QR code in the camera display.
- Step 3** Tap through and accept the Android setup screens.
The phone registers to the Cisco Unified Communications Manager and, if available, downloads the JSON configuration files, if DHCP points to the Cisco Unified Communications Manager.
-

Related Topics

- [Reset to factory default through the phone settings](#)
- [Generate a QR code to initialize phones](#), on page 4
- [Create encrypted phone configuration file](#), on page 5

Create encrypted phone configuration file

With the Cisco Wireless Phone Configuration Management tool, you can generate and save as many different configuration files that you need for different groups within your organization.

You can use the default settings for all apps, or you can change the app settings. Each setting has a blue info  icon that you can hover over for more information. When you make a change to a setting, a blue dot  appears to the left of the setting's blue info icon.

Before you begin

- Based on your organization's needs, determine which apps and settings you want to allow and disallow on the phone.
- Ensure that the apps that you want to include on the smart launcher are already installed on the phone.

Procedure

Step 1

From any browser, open the [Cisco Wireless Phone Configuration Management tool](#) to the **Deployment Configuration** tab.

Step 2

From Choose Application, select  **Smart Launcher** and set these parameters.

- **Set Allow-List of Applications:** Include the apps that you want to appear on the smart launcher. Use a comma-separated list of the app package names with no spaces.

Note By default, in the Cisco Wireless Phone Configuration Management tool, the following apps are set as allowed:

com.cisco.phone,com.cisco.ptt,com.cisco.emergency,com.cisco.webapi,com.cisco.wx2.android.

- **Set Title of Launcher Application:** Add a title to display on the smart launcher with multiple apps. The title doesn't appear if you have a single app on the smart launcher. Use up to 25 characters in the title. By default, the title is Smart Launcher. For example, add your company name or department.

Step 3

From Choose Application, select  **Device Policy Controller** and set the parameters.

- **Disallow These Apps:** Include the apps that you don't want to be accessible on the phone. Use a comma-separated list of the app package names without spaces.

Caution Don't include the Cisco Phone app on this list.

Make sure that none of the applications in the **Smart Launcher** allowed list are in this disallowed list, or the apps won't appear on the smart launcher home screen.

Note By default, in the Cisco Wireless Phone Configuration Management tool, the following apps are set as **com.google.android.youtube,com.google.android.googlequicksearchbox,com.android.soundrecorder**

- **Wi-Fi Profile:** Add up to five Wi-Fi profiles: WPA2-Personal or WPA2-Enterprise with EAP method of either:









- PEAP with MSCHAPv2 or GTC
- TTLS with GTC, PAP, MSCHAP or MSCHAPv2

Note Cisco Wireless Phone Configuration Management tool supports PEM certificates. When you copy and paste, don't include the certificate header, footer, white space, or new lines.

Step 4

From Choose Application, select, and configure each of the following Cisco apps as required by your organization.

Note If you want to accept all the default app settings, you don't need to make any changes. For more details about these Cisco app settings, see [Cisco app configuration](#).

-  **Barcode**
-  **Battery Life**
-  **Buttons**
-  **Custom Settings**
-  **PTT**
-  **Emergency**
-  **Call Quality Settings**
-  **Web API**

Step 5 Click **Export**.

Step 6 Check the **Encrypt Configuration** check box.

Note Don't use unencrypted files on your production server.

Step 7 Click **Export**.

The Cisco Wireless Phone Configuration Management tool export creates a zip file that contains three files.

Step 8 Save a copy of the zip file so that you can reuse or update the configuration file as needed.

Caution You can rename the zip file, if needed. But, if you plan on updating the configuration file later, keep a copy of the intact zip file without the inner files renamed.

Related Topics

[Cisco app package names](#)



[Preinstalled Android apps](#), on page 7

[Update existing configuration file](#), on page 9

[Product Specific Configuration Layout fields](#)

[Cisco Wireless Phone Configuration Management tool for Cisco app configuration](#)

Preinstalled Android apps

You can set these preinstalled Android apps to be either allowed or disallowed on the phones through the Cisco Wireless Phone Configuration Management tool **Smart Launcher**  and **Device Policy Controller**  apps.

The following table lists the preinstalled Android apps that are, by default, set to disallowed in the **Device Policy Controller**.

Table 1: Default preinstalled Android apps disallowed in the Device Policy Controller

Default disallowed Android apps	App package name
Chrome	com.android.chrome
Digital Wellbeing	com.google.android.apps.wellbeing
Google	com.google.android.googlequicksearchbox
Google TV	com.google.android.videos
Maps	com.google.android.apps.maps
Photos	com.google.android.apps.photos
Play Store	com.android.vending
Sound Recorder	com.android.soundrecorder
YouTube	com.google.android.youtube

You can also set these common preinstalled Android apps to the allowed or disallowed lists.

Table 2: More preinstalled apps

Preinstalled app	App package name
Calculator	com.google.android.calculator
Calendar	com.google.android.calendar
Camera	com.google.android.GoogleCamera
Clock	com.google.android.deskclock
Contacts	com.google.android.contacts
Drive	com.google.android.apps.docs
Duo	com.google.android.apps.tachyon
Files	com.marc.files
Gmail	com.google.android.gm
Keep Notes	com.google.android.keep
Webex	com.cisco.wx2.android
YT Music	com.google.android.apps.youtube.music

You can also install other Android apps to the phone, as needed.

Upload the phone configuration file to Cisco Unified Communications Manager

Before you begin

Create the encrypted phone configuration zip file with Cisco Wireless Phone Configuration Management tool.

Procedure

- Step 1** Extract the contents of the encrypted phone configuration zip file. The zip file contains three files:
- **config.json.enc**—Contains the phone configuration to import into Cisco Unified Communications Manager.
 - **key.txt**—Contains the encryption key to decrypt the **config.json.enc** file.
 - **config.json.react.enc**—Contains the configuration format for the Cisco Wireless Phone Configuration Management tool, which is used if you import the file.
- Note** Once you extract the zip file, you can rename the `config.json.enc` before you upload it to Cisco Unified Communications Manager. We recommend that you do this if you plan on having multiple configurations for various devices.
- Step 2** Sign in to Cisco Unified Communications Manager Administration.
- Step 3** Add the name of the `config.json.enc` file to the **Enterprise Mobility Management (EMM) Alternative Configuration** field in the Product Specific Configuration Layout pane.
- Note** If you renamed the `config.json.enc` file, make sure to use the new name.
- Step 4** Add the key in the `key.txt` file to the **Enterprise Mobility Management (EMM) Alternative Configuration Encryption Key** field in the Product Specific Configuration Layout pane.
- Note** You can also use bulk administration to set the key across the device types.
- Step 5** Add the `config.json.enc` file to all TFTP nodes running TFTP Services, and restart the TFTP services.
-

Related Topics

[Product Specific Configuration Layout fields](#)

Update existing configuration file

If you want to update an existing configuration file, you can import the existing configuration zip file in to the Cisco Wireless Phone Configuration Management tool, make the changes, and export a new configuration zip file.

Before you begin

If you want to keep a copy of the original configuration file, copy the intact zip file and rename it.



Caution Don't extract and rename the files within the zip, and then rezip the files.

Procedure

- Step 1** Open the [Cisco Wireless Configuration Deployment](#) tool.
 - Step 2** In the Deployment Configuration tab, click **Import**.
 - Step 3** Add the existing configuration zip file and click **Import**.
 - Step 4** Update the apps and settings.
 - Step 5** Click **Export** to create a new configuration zip file.
 - Step 6** Follow the steps to upload the new encrypted phone configuration file to Cisco Unified Communications Manager.
-

Related Topics

- [Create encrypted phone configuration file](#), on page 5
- [Upload the phone configuration file to Cisco Unified Communications Manager](#), on page 9

Manual phone configuration


You can manually configure the phones if you don't use an Enterprise Mobility Management (EMM) application and QR code, or the JSON configuration file and QR code from the Cisco Wireless Phone Configuration Management tool.

Wi-Fi profile configuration

For an out of box or factory reset phone, you configure the Wi-Fi network through the startup wizard or select **Set up offline**. How you configure the phone offline depends on whether the Wi-Fi network is either:

- Broadcasted
- Nonbroadcast or hidden

Add the phone to a broadcasted Wi-Fi network

You add the phone to a broadcasted Wi-Fi network through the startup wizard, or offline through the **Settings**  app.

Before you begin


Get the following information about the Wi-Fi network from your administrator:

- Network name or Service Set Identifier (SSID)
- Network security mode:

- None
 - Pre-shared key (PSK)
 - Protected Extensible Authentication Protocol (PEAP)
 - Extensible Authentication Protocol (EAP) Transport Layer Security (EAP-TLS)
 - EAP Tunneled Transport Layer Security (EAP-TTLS)
- PIN or passkey for the security mode, if you use one

Check with your administrator to see if you need any certificates and arrange to install the certificates on your phone.

Procedure

- Step 1** Swipe up from the bottom of the phone's display to show the installed applications.
- Step 2** Tap the **Settings**  app.
- Step 3** Select **Network & internet > Wi-Fi**.
- Step 4** Tap the desired Wi-Fi network name.
- If the network doesn't have a security mode, the phone automatically connects to the Wi-Fi network.
- If the network security mode is PSK, enter the 8–63 ASCII or 64 Hex Passphrase.
- Step 5** For a network with a PEAP, EAP-TLS, or EAP-TTLS security mode, select the **EAP method**: PEAP, TLS, or TTLS.
- Step 6** For a network with an EAP-TLS security mode, select the desired **CA certificate** and **User certificate**.
- Step 7** For a network with an EAP-TTLS or PEAP security mode, select the **Phase 2 authentication** method and **CA certificate** option to use, and then enter the **Identity** and **Password**.
- Step 8** Tap **Connect**.
-

Add the phone to a nonbroadcast Wi-Fi network

Follow these steps to add your phone to a Wi-Fi network that is hidden or not broadcast.

Before you begin

Get the following information about the Wi-Fi network from your administrator:


- Network name or Service Set Identifier (SSID)
- Network security mode:
 - None
 - Wi-Fi Protected Access II (WPA2)-Personal: Pre-shared key (PSK)
 - WPA2-Enterprise with EAP method:

- Protected Extensible Authentication Protocol (PEAP)
- Extensible Authentication Protocol (EAP) Transport Layer Security (EAP-TLS)
- EAP Tunneled Transport Layer Security (EAP-TTLS)

- PIN or passkey for the security mode, if you use one

Check with your administrator to see if you need any certificates and arrange to install the certificates on your phone.

Procedure

- Step 1** Swipe up from the bottom of the phone's display to show the installed applications.
- Step 2** Tap the **Settings**  app.
- Step 3** Select **Network & internet > Wi-Fi**.
- Step 4** Tap **Add Network**.
- Step 5** Enter the desired Wi-Fi **Network name**.
- Step 6** Select the desired **Security**:
- For an open network, select **None**.
 - For a PSK enabled Wi-Fi network, select **WPA2- Personal** and enter the 8-63 ASCII or 64 HEX **Password**.
 - For an EAP enabled Wi-Fi network, select **WPA2-Enterprise**.
- Step 7** For a WPA2-Enterprise network, select the **EAP method**: PEAP, TLS, or TTLS.
- Step 8** For a network with an EAP-TLS security mode, select the desired **CA certificate** and **User certificate**.
- Step 9** For a network with an EAP-TTLS or PEAP security mode, select the **Phase 2 authentication** method and **CA certificate** option to use, and then enter the **Identity** and **Password**.
- Step 10** Under **Advanced options**, set **Hidden network** to **Yes**.
- You can also set the **Proxy** and **IP settings** as required.
- Step 11** Tap **Save**.
-

Configure a TFTP server

You must configure a TFTP server if your network doesn't provide DHCP option 150 or 66 for the Cisco Unified Communications Manager that you want to register to.







Note Configure the DHCP pool with option 150 or 66 if you want to use the automatic configuration method.

Before you begin

You need the following information:

- **Local Phone Unlock Password**, if the default password was updated
- IP address of the TFTP server

Procedure

- Step 1** Access the **Cisco Phone**  app.
- Step 2** Choose one of the following based on your phone's software version:
- For release 1.2(0), tap the **Overflow**  menu.
 - For release 1.3(0) or later, tap the **Drawer**  menu.
- Step 3** Choose one of the following based on your phone's software version:
- For release 1.2(0), select **Settings > Phone information > Security**.
 - For release 1.3(0) or later, select **User settings > Phone information > Security**.
- Step 4** Enter the **Local Phone Unlock Password**.
- The default password is ****#**.
- Step 5** To enable alternate TFTP servers, swipe the **Alternate TFTP** slider to the right .
- Step 6** Enter the TFTP server addresses and tap **OK**.
- Step 7** Tap the back arrow in the upper left corner twice to save your changes and exit the menu.
-

Configure a Call server mode

Cisco Wireless Phone 840 and 860 can operate in either UCM or WxC mode. The phone can be configured both automatically and manually. You can manually select the **UCM** or **WxC** in call server mode and for automatic configuration select **Auto detect**.



Usually, when you select **Auto detect** in Call server mode, the phone tries to connect to UCM using the pre-existing behavior. If the phone gets configuration from a UCM, the phone operates in UCM mode and WxC mode will be disabled. If the phone cannot get configuration from a UCM, the phone tries to get WxC configuration. UCM mode will be disabled if WxC configuration is received. If the phone cannot get configuration for either CUCM or WxC, the phone will retry the auto detection process with a preset backoff schedule.

Before you begin

You need the following information:

- **Local Phone Unlock Password**, if the default password was updated

Procedure

- Step 1** Access the **Cisco Phone**  app.
- Step 2** For release 1.6(0) or later, tap the **Drawer**  menu.
- Step 3** Select **User settings > Phone information > Security**.
- Step 4** Enter the **Local Phone Unlock Password**.
The default password is ****#**.
- Step 5** Choose one of the following options in the Call server mode.
- **Auto detect**
 - **UCM**
 - **WxC**
- Step 6** Tap the back arrow in the upper left corner twice to save your changes and exit the menu.
-